# AN APPARATUS FOR PROVIDING A SECURE PROCESSING ENVIRONMENT

**Publication number:** JP2002526822T

**Publication date:** 2002-08-20

**Inventor:**

**Applicant:**

**Classification:**

**- international:** ***G06F12/14; G06F21/00; G06F21/06; G06F21/22; G06F21/24; H04L9/10;*** **G06F12/14; G06F21/00; G06F21/22; H04L9/10;** (IPC1-7): G06F12/14; G06F1/00; H04L9/10

**- European:** G06F12/14B; G06F21/00N1C3; G06F21/00N1C4; G06F21/00N1D; G06F21/00N1V3; G06F21/00N7P5H; G06F21/00N9A

**Application number:** JP20000572741T 19980925

**Priority number(s):** WO1998US20083 19980925

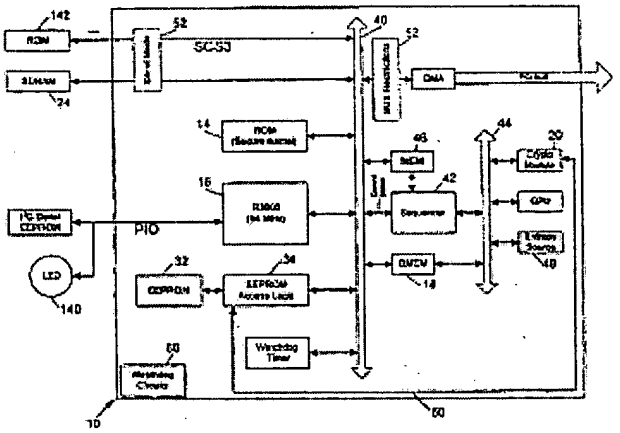
**Also published as:**

WO0019299 (A1)
EP1032869 (A1)
EP1032869 (A0)
CA2309627 (A1)
AU743775B (B2)

Report a data error here

Abstract not available for JP2002526822T
Abstract of corresponding document: **WO0019299**

An apparatus for providing a secure processing environment is disclosed. In one embodiment, the apparatus includes a read/write memory for storing encrypted information. It also includes a processor, a cipherer and an authenticator. The cipherer is in communication with the read/write memory for receiving encrypted information therefrom and is configured to decrypt the encrypted information into decrypted information to be returned to the memory for subsequent use by the processor. The authenticator authenticates the decrypted information prior to use by the processor and reauthenticates the information prior to re-encryption by the cipherer.




Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－526822
（P2002－526822A）
(43)公表日　平成14年８月20日(2002.8.20)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　12/14 | ３２０ | Ｇ０６Ｆ　12/14 | ３２０Ａ | ５Ｂ０１７ |
| | | | ３２０Ｂ | ５Ｂ０７６ |
| 1/00 | | 9/06 | ６６０Ｌ | ５Ｊ１０４ |
| Ｈ０４Ｌ　9/10 | | Ｈ０４Ｌ　9/00 | ６２１Ａ | |

審査請求　有　　予備審査請求　未請求(全 77 頁)

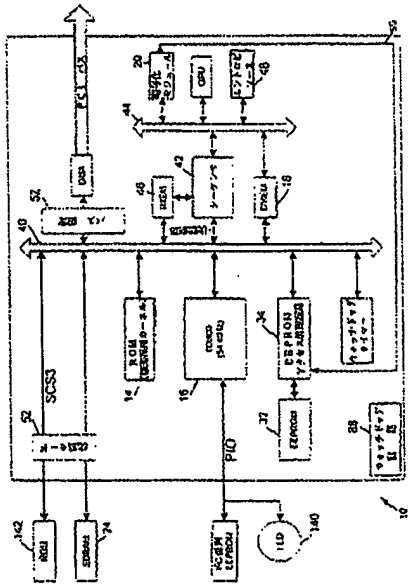
(21)出願番号　特願2000－572741(P2000－572741)
(86)(22)出願日　平成10年９月25日(1998.9.25)
(85)翻訳文提出日　平成12年５月25日(2000.5.25)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／２００８３
(87)国際公開番号　ＷＯ００／１９２９９
(87)国際公開日　平成12年４月６日(2000.4.6)

(71)出願人　ヒューズ・エレクトロニクス・コーポレーション
アメリカ合衆国、カリフォルニア州　90245、エル・セグンド、ノース・セプルベーダ・ブールバード　200
(72)発明者　カサニョール、ロバート・ディー
アメリカ合衆国、メリーランド州　20904　シルバー・スプリング、アラバスター・ドライブ　1904
(74)代理人　弁理士　鈴江　武彦　（外４名）

最終頁に続く

(54)【発明の名称】　セキュリティ処理環境を提供するための装置

(57)【要約】
機密保持された処理環境を提供する装置が開示されている。１実施形態において、装置は暗号化された情報を記憶するための読取り／書込みメモリを含んでいる。それはまた、プロセッサ、暗号化装置および認証装置を含んでいる。暗号化装置は読取り／書込みメモリと通信しており、それらから暗号化された情報を受取って、この暗号化された情報を解読された情報にするように構成されており、この解読された情報がプロセッサによる後続的な使用のためにメモリに戻される。認証装置は、解読された情報をプロセッサが使用する前に認証し、この情報を暗号化装置が再度暗号化前に再度認証する。



【特許請求の範囲】

【請求項１】　情報を記憶する読取り／書き込みメモリと、

読取り／書き込みメモリと共同して、そこから情報を読取り、そこに情報を書込む第１のプロセッサと、

読取り／書き込みメモリと通信し、暗号化された情報を選択的に解読して解読された情報にし、第１のプロセッサが後で使用するために解読された情報を読取り／書き込みメモリに供給するように構成されている暗号化装置と、

第１のプロセッサによって使用される前に、解読された情報を認証する認証装置とを具備している機密保持された処理環境を提供する装置。

【請求項２】　認証装置は、読取り／書込みメモリから受取った解読された情報を再度認証し、暗号化装置は、解読され、再度認証された情報を選択的に暗号化して再度暗号化された情報にするように構成されている請求項１記載の装置。

【請求項３】　暗号化装置は、記憶装置に後でエクスポートするために、再度暗号化された情報を読取り／書込みメモリに戻す請求項２記載の装置。

【請求項４】　暗号化装置は、修正情報をマスクするためにその元の暗号化された形態とは異なるように解読され再度認証された情報を再度暗号化する請求項２記載の装置。

【請求項５】　暗号化装置は、修正情報をマスクするためにキーサイクリングを使用する請求項４記載の装置。

【請求項６】　暗号化装置は修正情報をマスクするためにホワイトニングプロセスを使用し、ホワイトニングプロセスはホワイトニングキーを使用し、ホワイトニングキーが循環される請求項４記載の装置。

【請求項７】　再暗号化前に解読された情報を再度認証するために使用される認証データは、後で解読された情報を認証する時に使用するために、読取り／書込みメモリ中に記憶される請求項２記載の装置。

【請求項８】　再度暗号化された情報を選択的に記憶する外部メモリをさらに具備している請求項２記載の装置。

【請求項９】　第１のプロセッサは、カーネル動作モードおよびユーザ動作

モードを有しており、カーネルモードとユーザモードとは別個のセキュリティセルを規定している請求項１記載の装置。

【請求項１０】　第１のプロセッサは、ユーザ動作モードで機密保持されていないソフトウェアを実行し、カーネル動作モードで安全なソフトウェアを実行する請求項９記載の装置。

【請求項１１】　暗号化装置および読取り／書込みメモリと通信し、それによって読取り／書込みメモリに記憶されている情報の解読および再暗号化を選択的に開始する第２のプロセッサをさらに具備している請求項１記載の装置。

【請求項１２】　暗号化装置は、認証装置を含んでいる請求項１１記載の装置。

【請求項１３】　暗号化された情報は、暗号化されたプロセッサ命令を含んでいる請求項１記載の装置。

【請求項１４】　暗号化された情報は、暗号化されたデータを含んでいる請求項１記載の装置。

【請求項１５】　暗号化された情報は、セクションにセグメント化されている請求項１記載の装置。

【請求項１６】　各セクションは、独立に暗号化され、認証される請求項１５記載の装置。

【請求項１７】　不揮発性メモリと、この不揮発性メモリに含まれているデータへのアクセスを制御し、不揮発性メモリに選択的にアクセスし、アクセスされたデータに固有のプロパティを解析することによって、不揮発性メモリに含まれてるデータが機密データを含んでいるか否かを決定する論理回路とをさらに具備している請求項１記載の装置。

【請求項１８】　論理回路は、予め定められた特性を有しているアクセスされたデータ中のデータブロックを識別し、その識別されたデータブロックをカウントし、このカウントをしきい値と比較することによって、不揮発性メモリに含まれているデータが機密データを含んでいるか否かを決定する請求項１７記載の装置。

【請求項１９】　各データブロックはビットを含み、予め定められた特性は

予め規定された論理状態を含んでいる請求項１８記載の装置。

【請求項２０】　各データブロックは複数のビットを含み、予め定められた特性は２進値の範囲内に入る２進値を含んでいる請求項１８記載の装置。

【請求項２１】　論理回路は、第１のプロセッサを備えている請求項１７記載の装置。

【請求項２２】　論理回路を暗号化装置に直接接続するキー分離回路をさらに具備している請求項１７記載の装置。

【請求項２３】　不揮発性メモリはキーを記憶し、キー分離回路がキーを暗号化装置に供給する請求項２２記載の装置。

【請求項２４】　論理回路、キー分離回路および暗号化装置は、閉じたシステムを規定している請求項２２記載の装置。

【請求項２５】　第１のプロセッサ、読取り／書込みメモリおよび暗号化装置は、集積回路上に埋込まれている請求項１記載の装置。

【請求項２６】　集積回路は外部デバイスに装置を接続するためのピンを含んでおり、また、機密保持された環境外へのセンシチブな情報の公開を回避するようにピンを選択的にディスエーブルにするためのサイレンシング回路をさらに具備している請求項２５記載の装置。

【請求項２７】　タンパーするための集積回路を監視するように構成されたウォッチドッグ回路をさらに具備している請求項２５記載の装置。

【請求項２８】　暗号化された情報を外部ソースから選択的に受取る入力をさらに具備している請求項２５記載の装置。

【請求項２９】　第１のプロセッサと共同して複数のセキュリティセルを維持するメモリ管理装置をさらに具備している請求項１記載の装置。

【請求項３０】　暗号化装置は暗号化モジュールを含んでいる請求項１記載の装置。

【請求項３１】　解読された情報の認証は対応している暗号化された情報を認証することによって行われる請求項１記載の装置。

【請求項３２】　第１の記憶容量を有し、暗号化された情報を記憶する外部メモリにより使用される、機密保持された処理環境を提供するための集積回路に

おいて、

第１の記憶容量より少ない第２の記憶容量を有している揮発性メモリと、

暗号化された情報を外部メモリと揮発性メモリとの間で選択的にインポートおよびエクスポートするためのインポート／エクスポート手段と、

機密保持された環境内において揮発性メモリから受取った暗号化された情報を解読して解読された情報にし、機密保持された環境内において解読された情報を再び暗号化して暗号化された情報に戻すための暗号化手段と、

機密保持された環境内において解読された情報を処理し、インポート／エクスポート手段と共同して、第２の記憶容量の超過を回避するために解読された情報を外部メモリと揮発性メモリとの間で選択的にインポートおよびエクスポートするプロセッサとを具備している集積回路。

【請求項３３】　暗号化手段は、解読された情報に対応している暗号化された情報が外部メモリからインポートされた場合に第１の形態を有し、また、外部メモリにエクスポートされた場合には、対応している解読された情報が不変のままであるときにも、第１の形態とは異なる第２の形態を有するように情報を暗号化する請求項３２記載の集積回路。

【請求項３４】　解読手段は、暗号化された情報を第１のホワイトニングキーを使用して解読し、解読された情報を第１のホワイトニングキーとは異なる第２のホワイトニングキーを使用して暗号化する請求項３３記載の集積回路。

【請求項３５】　第２のホワイトニングキーを発生する暗号的に強い疑似ランダム数発生器をさらに具備している請求項３４記載の集積回路。

【請求項３６】　機密保持された環境内において解読された情報を認証するための手段をさらに具備している請求項３２記載の集積回路。

【請求項３７】　認証するための手段は、外部メモリからインポートした後に解読された情報を認証し、外部メモリにエクスポートする前に解読された情報を再度認証する請求項３６記載の集積回路。

【請求項３８】　機密保持動作を行うために集積回路において使用される、集積回路をタンパーチェックするための方法において、

事象を検出し、

タンパーが発生しているか否かを決定するために集積回路の１以上の素子に関して組込み自己試験を実行し、

この組込み自己試験によってタンパーの発生が示された場合には、集積回路の１以上の動作を制限するステップを含んでいるタンパーチェック方法。

【請求項３９】　キー材料を記憶している予め規定されたメモリがアクセスされることができないように集積回路に関連したプロセッサをリセット状態に保持し、

１以上の素子が組込み自己試験に合格した場合にはリセット状態からプロセッサを解放し、

１以上の素子が組込み自己試験に失敗した場合には、プロセッサをリセット状態に保持するステップをさらに含んでいる請求項３８記載の方法。

【請求項４０】　前記１以上の素子はメモリを含んでいる請求項３８記載の方法。

【請求項４１】　前記１以上の素子は論理回路を含んでいる請求項３８記載の方法。

【請求項４２】　前記事象はリセット事象を含んでいる請求項３８記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、一般にプログラムされたデバイスのセキュリティに関し、とくに、機密データならびにソフトウェア等の機密プログラムステップの少なくとも一方を処理するための機密保持された環境を提供する装置に関する。

【従来の技術】

データおよびプログラムされた命令（たとえば、ソフトウェア）の少なくとも一方の値段は、関心を持った大衆が一般的に入手できる可能性に依存していることが多い。たとえば、データまたはプログラムされた命令の形態の情報がインターネット上で無料で入手できるようにされている場合、無料で容易に入手できるものにお金を払う者はほとんどいないため、その情報の市場価格はゼロにむかって急落する。したがって、機密情報の代金を支払った購入者以外のすべてに関してデータおよびプログラムされた命令の少なくとも一方のセキュリティを維持することが望ましいことが以前から知られている。

【０００２】

情報へのアクセスを制限することによってその情報から派生する価値の概念が活用されている多数の状況が存在する。たとえば、ケーブルテレビジョンネットワークのような条件付きアクセス放送ネットワークや、近年では直接衛星放送ネットワークが代金を支払っている加入者に対して放送された情報へのアクセスを制限するという前提に基づいている。最近は、放送されたデータへのアクセスを制限するという考えが、ヒューズ・ネットワーク・システムズ社のディレクＰＣ（商標名）プロダクトによってコンピュータネットワーキング状況に拡張されている。このディレクＰＣ（商標名）プロダクトは、インターネットからの情報配信を促進するための手段として衛星を介して要求された情報を要求したコンピュータデバイス（代表的に、パーソナルコンピュータ）に放送する。

【０００３】

このような放送システムのほとんどが、放送された情報へのアクセスを制御するために１以上の暗号技術を使用している。たとえば、このようなシステムの

ほとんどが放送されたデータを数学的アルゴリズムに基づいて暗号化するために１以上のキーを使用しており、この数学的アルゴリズムのために、データを暗号化するために使用されたキーの知識がなければ、相当の時間を費やさない限り、データの解読は非常に難しいものとなっている。ここにおいて、文献全体が参考文献とされている文献（Schneier,Applied Cryptography,(Second Ed.1996)）には、放送された情報を暗号化するために頻繁に使用されているデータ暗号化規格（ＤＥＳ）アルゴリズムの説明を含む多数のこのような暗号技術の説明が含まれている。

【０００４】

情報のセキュリティを保護する必要性は、放送環境だけに制限されない。たとえば、商業的観点から、パーソナルコンピュータによって局所的に処理されるために情報の機密性を維持することが重要な多くの応用が存在する。たとえば、いくつかの適用では、機密データの処理を許す一方で外界に対するそのデータのセキュリティを維持することが望ましい。これは一例に過ぎず、それに限定されるものではない。別の例をあげると、いくつかの例において、プログラムされた命令（たとえば、ソフトウェア）のプロセッサ内における機密保持された実行が、解読された命令自身へのそのプロセッサ外からのアクセスを許さずに可能であることが望ましい。

【０００５】

情報のセキュリティを維持するための種々のデバイスが開発されている。しかしながら、これらのデバイスによって保護された機密情報には非常に高い商業価値があることが多いため、一般に“ハッカー”と呼ばれる者達の侵入技術(sub-culture) も発達してきている。このような者達は、機密情報の商業価値を奪取(usurp) するためにかなりの時間を費やしてこれらのデバイスのセキュリティ手段を打破または“ハック”しようとする。ハッカーがこうした行為に成功するレベルは多様である。したがって、ハッカーに対して既知のデバイスより高いレベルのセキュリティを実現する、情報処理用の機密環境を提供するための改善されたもっとフレキシブルな装置が必要とされている。さらに、機密デバイスに固有のメモリ制限を克服し、そのソフトウェアがフィールドでアップグレードされる

ことのできる装置が必要である。

【０００６】

機密は完全にシステムのキーの中に存在しなければならないことは一般に認められている暗号方式のよく知られた前提である。換言すると、機密と考えられるデバイスについて、キー以外のシステムに関する全情報にアクセスしたアタッカーが妥当な時間内に暗号化された情報を解読することが不可能でなければならない。したがって、キー材料のセキュリティは、機密環境を提供するデバイスにおいて最も重要である。

【０００７】

そのため、一般に、情報の暗号化、解読およびそのセキュリティの維持の少なくとも１つを行うためのデバイスは、キー材料およびその他の、恐らく高度の機密にかかわるデータを記憶するあるタイプの機密メモリを含んでいる。そのキー材料へのアクセスを制御するために、機密メモリへのアクセスを信頼できるソフトウェアおよびハードウェアコンポーネントの少なくとも一方に制限することが要求されることが多い。とくに、キー材料を記憶しているメモリがアドレスされることのできる時機、人物、および環境を制限することがしばしば必要である。

【発明が解決しようとする課題】

メモリへのアクセスの制限に関する１つの問題は、試験可能なことである。別の問題は、工場での初期プログラミングを依然として許しながらフィールド配備ユニットへのアクセスを制限することである。デバイスをフィールドに解放する前にメモリが適切に機能することを検査するために、メモリへの完全読取り／書込みアクセスを行うことがしばしば要求される。さらに、このようなアクセスは典型的に、デバイスが完全に、あるいはほぼ完全に構成された後で行われなければならない。その結果、このようなデバイスはしばしば試験モードを含み、このモードにおいて、デバイスは、ある状態または事象の発生時にそれが試験モード中であると判断し、メモリへの全読取り／書込みアクセスを許す。ハッカーがキー材料を含むデバイスを騙して、これを試験モードにすることができれば、記憶されたキー材料に対してまともにアクセスすることが可能となり、それによって

デバイスのセキュリティは完全に危険にさらされる。

【０００８】

いくつかの従来技術の方法において、メモリ、またはアンチヒューズデバイス等に記憶された１以上のモードビットは、そのメモリが機密データを含んでいるか否か、およびそのメモリが試験モード中であるか否かの少なくとも一方を規定する。このモードビットは、メモリ中のデータ上の簡単なチェックサムとして構成されてもよい。換言すると、モードビットは、メモリに記憶されたあるデータまたは全データのある数学的関数に等しく設定されてもよい。モードビットを規定するために伝統的な方法のどれを使用しても、ハッカーがモードビットの状態を変更すれば、メモリを試験モードにさせることが可能となり、それによってメモリが含んでいるキー材料は完全に危険にさらされる。したがって、メモリに記憶されたモードビットまたはメモリに記憶されたチェックサム値に依存しない、機密データをそのメモリが含んでいるか否かを判断して決定するための改善された方法および装置を提供することが望ましい。

【課題を解決するための手段】

本発明の特徴によると、機密処理環境を提供するための装置が提供される。装置は、情報を記憶するための読取り／書込みメモリと、この読取り／書込みメモリと共同し、そこから情報を読取ると共にそこに情報を書込むための第１のプロセッサと、読取り／書込みメモリと通信する暗号化装置とを含んでいる。この暗号化装置は、暗号化された情報を選択的に解読して解読された情報を生成し、この解読された情報を第１のプロセッサによる後続的な使用のために読取り／書込みメモリに供給するように構成されている。さらに、装置は、解読された情報をプロセッサが使用する前に認証する認証装置を具備している。

【０００９】

いくつかの実施形態において、認証装置は読取り／書込みメモリから受取った解読された情報を再度認証し、暗号化装置はこの解読された再度認証された情報を再度暗号化された情報に選択的に暗号化するように構成されている。このような実施形態において、暗号化装置は随意に、再度暗号化された情報を読取り／書込みメモリに戻して、その後に記憶デバイスにエクスポートしてもよいし、あ

るいは随意に再度暗号化された情報を直接エクスポートしてもよい。また、このような実施形態において、暗号化装置は、解読された再度認証された情報を再度暗号化し、結果的にそれが修正情報をマスクするように元の暗号化された形態とは異なっていることが好ましい。このような実施形態では、暗号化装置は修正情報をマスクするためにキーサイクリングおよび、またはホワイトニングキーのサイクリングを使用する。

【００１０】

いくつかの実施形態では、解読された情報を再度暗号化する前に再度認証するために使用される認証データは、後で解読された情報の認証時に使用するために読取り／書込みメモリに記憶される。

【００１１】

いくつかの実施形態では、第１のプロセッサはカーネル（核）動作モードおよびユーザ動作モードを有しており、カーネルモードおよびユーザモードは別々のセキュリティセルを規定している。このような実施形態において、第１のプロセッサは、ユーザ動作モードで非機密ソフトウェアを実行し、カーネル動作モードで機密ソフトウェアを実行することが好ましい。

【００１２】

いくつかの実施形態において、装置は第２のプロセッサを具備している。第２のプロセッサは、暗号化装置および読取り／書込みメモリと通信し、それによって読取り／書込みメモリに記憶された情報の選択的な解読および再暗号化を開始する。このようないくつかの実施形態では、暗号化装置は認証装置を含んでいる。

【００１３】

いくつかの実施形態において、装置はさらに、不揮発性メモリと、この不揮発性メモリに含まれているデータへのアクセスを制御するための論理回路とを具備し、論理回路が不揮発性メモリに選択的にアクセスし、アクセスされたデータに固有のプロパティを解析することによって不揮発性メモリに含まれているデータが機密データを含んでいるか否かを決定する。このようないくつかの実施形態において、論理回路は、予め定められた特性を有しているアクセスされたデータ

中のデータブロックを識別し、識別されたデータブロックをカウントし、そのカウントをしきい値と比較することによって不揮発性メモリに含まれているデータが機密データを含んでいるか否かを決定する。このようないくつかの実施形態では、各データブロックはビットを含み、予め定められた特性は予め規定された論理状態を含んでいてもよい。その代わりに、各データブロックは複数のビットを含み、予め定められた特性はある範囲の２進値内に入る２進値を含んでいてもよい。

【００１４】

不揮発性メモリを上述のように使用するいくつかの実施形態において、論理回路を暗号化装置に直接接続するキー分離回路が設けられている。いくつかのこのような実施形態において、不揮発性メモリはキーを記憶し、キー分離回路がキーを暗号化装置に供給する。上述の実施形態の任意のものにおいて、論理回路、キー分離回路および暗号化装置は、閉じたシステムを規定することが好ましい。

【００１５】

いくつかの実施形態において、不揮発性メモリ、第１のプロセッサ、読取り／書込みメモリおよび暗号化装置は、集積回路上に埋込まれている。このような実施形態において、集積回路は外部デバイスに装置を接続するためのピンを含み、装置は、機密保持された環境外へのセンシチブな情報の公開を回避するようにピンを選択的に使用禁止状態（ディスエーブル）にするためのサイレンシング回路、およびタンパーするための集積回路を監視するように構成されたウォッチドッグ回路の少なくとも一方をさらに含んでいる。

【００１６】

いくつかの実施形態において、装置は、第１のプロセッサと共同して複数のセキュリティセルを維持するためのメモリ管理装置を含んでいる。

【００１７】

いくつかの実施形態において、暗号化装置は暗号化モジュールを含んでいる。

【００１８】

上記の実施形態の任意のものにおいて、認証は、解読前に暗号化された情報

を認証することによって行われてもよい。

【００１９】

上記の実施形態の任意のものにおいて、暗号化された情報は、暗号化されたプロセッサ命令および、または暗号化されたデータを含んでいてもよい。

【００２０】

上記の実施形態の任意のものにおいて、暗号化された情報は、セクションにセグメント化されてもよい。このような実施形態において、セグメントは独立に暗号化され、認証されることが好ましい。

【００２１】

本発明の別の特徴によると、機密保持された処理環境を提供するための集積回路が外部メモリにより使用されるために提供される。その装置は、外部メモリの記憶容量より少ない記憶容量を有する揮発性メモリを含んでいる。装置は、暗号化された情報を外部メモリと揮発性メモリとの間で選択的にインポートおよびエクスポートするためのインポート／エクスポート手段と、機密保持環境内において揮発性メモリから受取った暗号化された情報を解読して解読された情報を生成し、機密保持環境内において解読された情報を再び暗号化して暗号化された情報にするための暗号化手段とをさらに含んでいる。さらに、装置は、機密保持環境内において解読された情報を処理するためのプロセッサを含んでいる。このプロセッサは、インポート／エクスポート手段と共同して、第２の記憶容量の超過を回避するために解読された情報を外部メモリと揮発性メモリとの間で選択的にインポートおよびエクスポートする。

【００２２】

いくつかの実施形態において、暗号化手段は解読された情報に対応している暗号化された情報が外部メモリからインポートされた場合には第１の形態を有し、また、外部メモリにエクスポートされた場合には、対応している解読された情報が不変のままである場合にも、第１の形態とは異なる第２の形態を有するように情報を暗号化する。いくつかのこのような実施形態において、暗号化手段は、暗号化された情報を第１のホワイトニングキーを使用して解読し、解読された情報を第１のホワイトニングキーとは異なる第２のホワイトニングキーを使用して

暗号化する。いくつかのこのような実施形態では、装置は、第２のホワイトニングキーを発生する暗号法的に強い疑似ランダム数発生器を具備している。

【００２３】

いくつかの実施形態において、装置は、機密保持された環境内において解読された情報を認証する手段を具備している。いくつかのこのような実施形態において、認証する手段は、外部メモリからインポートした後に解読された情報を認証し、暗号化して外部メモリにエクスポートする前に、解読された情報を再度認証する。

【００２４】

本発明の１特徴によると、機密保持された動作を行うために集積回路をタンパーチェックする方法が提供される。この方法は、事象を検出し、タンパーが発生しているか否かを決定するために集積回路の１以上の素子に関して組込み自己試験を実行し、この組込み自己試験によってタンパーの発生が示された場合には、集積回路の１以上の動作に対して制限を課すステップを含んでいる。

【００２５】

いくつかの実施形態において、この方法はまた、キー材料を記憶した予め規定されたメモリがアクセスされることができないように、集積回路に関連したプロセッサをリセット状態に保持し、１以上の素子が組込み自己試験に合格した場合はリセット状態からプロセッサを解放し、１以上の素子が組込み自己試験に失敗した場合には、プロセッサをリセット状態に保持するステップを含んでいる。いくつかのこのような実施形態において、１以上の素子は予め規定されたメモリおよび論理回路の少なくとも一方を含んでいる。

【００２６】

上記の実施形態の任意のものにおいて、検出された事象は、リセット事象を含んでいてもよい。

【発明の実施の形態】

その他の特徴および利点は、特許請求の範囲に記載され開示されている装置に固有であり、以下の詳細な説明および添付図面から当業者に明らかにされるであろう。

図１には、使用可能な１つの環境における、すなわちパーソナルコンピュータ（示されていない）で使用されるディレクＰＣ（商標名）モジュール12上における本発明の教示にしたがって構成された装置10が概略的に示されている。以下詳細に説明するように、装置10はセンシチブな(sensitive) 情報を処理するための機密保持された環境を提供するように構成されている。この説明および添付された特許請求の範囲において一貫して使用されている“情報”という用語は、データ、プログラムされた命令（たとえば、ソフトウェア、ファームウェア）あるいはその両者を指している。装置10はディレクＰＣ（商標名）製品において使用可能であるが、当業者は、装置10が任意の特定の環境における使用あるいは任意の特定の用途での使用に限定されないことを理解するであろう。逆に、示されている装置10は、本発明の技術的範囲を逸脱することなく、それが提供する増加された処理セキュリティから利益を得る任意の用途または環境において使用されることが可能である。たとえば、それは、スマートカード適用においてとくに有効である。さらに、装置10は図１において適用特定集積回路（ＡＳＩＣ）として構成されたものとして示されているが、当業者は、装置10が集積回路として構成される必要がないことを容易に認識するであろう。

【００２７】

以下説明するように、示されている装置10は、センシチブな情報の内容が装置10外に露出されることなく、解読、処理および再暗号化されることのできる機密保持された環境を提供するように構成されている。（ここで使用されている“解読された”とは、１以上の暗号層が除去されたことを意味する。当業者によって理解されるように、ここで使用されている“解読された情報”は随意に依然として暗号化されていてもよいが、完全に暗号が解かれた形態に１ステップ以上近付いたものである。たとえば、バーサクリプト(VersaCrypt)環境は、暗号化されたＲＳＡ解読データのような別の暗号系を持込むために、あるいは別の暗号系にしたがって解読される過程で使用されることができる。）１つの観点で、示されている装置10は、センシチブな情報が機密保持された環境外に露出される場合には常に暗号化されることを厳密に確実にすることによってこのセキュリティを達成する。解読されたセンシチブな情報が装置10において利用可能であるときは常

に、外部デバイスによる装置10へのアクセスを阻止するようにセキュリティ手段が動作される。

【００２８】

いくつかの適用では、当然のことながら、情報を解読するために使用されるプロセスおよびキーの機密性を維持しながら解読された情報を装置10からエクスポートすることが望ましい。たとえば、データベースへのアクセスを計測ために使用されるソフトウェア計測適用では、認証されたユーザに適切に料金を請求してしまえば、彼等にデータベースの解読された内容を提供することが望ましい。このような適用において、装置10は、使用されるキー材料を隠しているデータの解読および解読中行われるプロセスのための機密保持された環境を提供する。

【００２９】

示されている装置10は、テレビジョン加入者放送システムのような条件付きデータアクセス適用において非常に有効であるが、装置10の最大限の能力は、条件付きソフトウェアアクセス適用においてより完全に使用される。このような適用において、示されている装置10は、解読された命令を機密保持された環境の外部に露出することなく、センシチブなソフトウェア（またはファームウェア）情報を解読し、実行し、再度暗号化することができる。暗号化されたソフトウェア（またはファームウェア）は、装置10に随意に記憶されてもよいし、あるいはメモリ制約のために、装置10の外部に記憶されてもよく、必要に応じて装置10に選択的にインポートされてもよい（まとめて、あるいはセグメントで）。いずれの場合も、以下説明するように、示されている装置10は大きい基板上の処理容量を有しているため、解読されたソフトウェア（またはファームウェア）の実行は完全に機密保持された環境において行われることができる。その結果、センシチブなソフトウェア（またはファームウェア）は、認証されていないエンティティによる使用のために、あるいは非適合(non-conformant)動作を誘導するために容易に変更され、あるいは著作権を侵害されることはできない。

【００３０】

暗号化されたソフトウェア（またはファームウェア）の実行により、装置10は情報をユーザが読出すことのできる形態で外部装置（たとえば、モニタ、プリ

ンタ、記憶装置等）に出力するが、出力情報を発生するソフトウェアは通常、装置10によって提供された機密保持された環境外に露出されない（もちろん、解読された形態で命令をエクスポートするために実行されるソフトウェア（またはファームウェア）中の命令なしで）。したがって、ソフトウェア（またはファームウェア）のセキュリティは、示されている装置10によって常に維持されている。以下説明するように、示されている装置10のこの特徴の有効な結果は、たとえばソフトウェア（またはファームウェア）が実際に使用される時間量に合わせられた使用量に基づいて、認可されたソフトウェア（またはファームウェア）のユーザが料金を請求されることのできるソフトウェア（またはファームウェア）計量を実施できることである。たとえば、示されている装置10は、当該ソフトウェア（またはファームウェア）の任意の部分が解読された形態で維持される時間量を監視するように構成されることができる。この監視によって収集されたデータは、ソフトウェア（またはファームウェア）使用の認可料金を課すために使用されることができる。ソフトウェア（またはファームウェア）を認可するこの方法は、アップグレードなしで、一回限りの(one-time)認可料金が請求される伝統的な方法とはっきり対照をなしている。

【００３１】

装置10の動作のあるもの（すなわち、“機密保持されたカーネル”）を規定するプログラムされた命令を記憶するために、装置10は不揮発性メモリ14（図２）を具備している。機密保持されたカーネルは、装置10内におけるリソース管理を担当している。それは以下に説明するセキュリティ制限の多くを実施する。不揮発性メモリ14に記憶された符号は暗号化されないことが好ましいが、当業者は、本発明の技術的範囲を逸脱することなく、暗号化された情報（たとえば、データまたはプログラムされた命令）が不揮発性メモリ14に記憶されることが可能なことを理解するであろう。不揮発性メモリ14は、本発明の技術的範囲を逸脱することなく多数の方法で構成可能なことが理解されるが、この好ましい実施形態では、プログラムされた命令を記憶した読出し専用メモリ（ＲＯＭ）によって構成されている。以下説明するように、装置10は、ホワイトニングを有するトリプルキー、トリプルＤＥＳ－ＣＢＣを使用して個々に暗号化されたバーサクリプト(V

ersaCrypt)アプレットにセグメント化されていることが好ましい機密保持されたソフトウェアを実行する。

【００３２】

情報を処理し、装置10の動作を制御するために、装置10はプロセッサ16（図２参照）を具備している。以下さらに詳細に説明するように、プロセッサ16の１つの機能は、２以上のセキュリティセルを実施することである。セキュリティセルの第１のものは、ここではカーネルモードセルと呼ばれており、センシチブな機密情報がアクセスされ、処理され、装置10の内部バス上で利用可能にされている場合には常に実施されることが好ましい。第２のセキュリティセルは、ここではユーザモードセルと呼ばれており、センシチブなデータへのアクセスが許可されない場合に実施される。カーネルモードが有効なとき、プロセッサ16は装置10内のハードウェアおよびソフトウェアリソースへのアクセスに対して何等制限を課さない。それはまた、以下説明するように、装置10によって実行されている動作および装置10によって処理されている情報の少なくとも一方を示すセンシチブな情報を装置10の外部ピンが暴露することを防止する。ユーザモードが実施されたとき、プロセッサ16は増強されたレベルの制限を装置10内の動作に与えるが、外的に可視である動作には制限を課さない。しかしながら、以下説明するように、あるハードウェア実施制限は、両セキュリティセルにおいて維持されることが好ましい。

【００３３】

装置10によって処理されるべき情報を一時的に記憶するために、装置10は揮発性の読取り／書込みメモリ18をさらに具備している。この読取り／書込みメモリ18は、プロセッサ16が必要に応じてメモリ18に含まれている情報の読取りおよびメモリ18への情報の書込みの両者を行うことができるように、プロセッサ16によってアドレス指定可能である。以下詳細に説明するように、動作において、装置10によって処理されるべき暗号化された情報は、最初に読取り／書込みメモリ18に書込まれる。したがって、１つの役割において、読取り／書込みメモリ18は暗号化された情報に対する記憶領域として機能する。

【００３４】

暗号化機能を行うために、装置10は、暗号化された情報を解読された情報に解読し、解読された情報を暗号化された情報に再度暗号化するための暗号化手段を具備している。これらの両機能は、機密保持された安全な環境内で行われる。当業者によって理解されるように、暗号化手段は、本発明の技術的範囲を逸脱することなく多数の異なった方式で構成されることができる。たとえば暗号化手段は、ソフトウェアまたはファームウェアを実行する専用ハードウェア回路またはプロセッサのような暗号化装置20によって構成されることができる。さらに、当業者は、暗号化装置20が本発明の技術的範囲を逸脱することなくよく知られている種々の暗号技術およびアルゴリズムの少なくとも一方を行うように構成されることが可能なことを理解するであろう。この好ましい実施形態において、暗号化装置20は、ここでは暗号化モジュールと呼ばれる専用ハードウェア回路20によって構成され、この暗号化モジュールは、適用の要求に応じて、（１）トリプルキー、トリプルＤＥＳ－ＣＢＣ暗号化および解読（トリプルキー、トリプルデータ暗号化規格／電子符号ブックモード暗号化／解読）、（２）トリプルキー、トリプルＤＥＳ外部ＣＢＣ（トリプルキー、外部暗号化ブロックチェイニングによるトリプルデータ暗号化規格）暗号化および解読、および（３）ＤＶＢ（デジタルビデオ放送）デスクランブルを行うことができる。

【００３５】

図２に示されているように、暗号化装置20は、読取り／書込みメモリ18と通信している。動作において、読取り／書込みメモリ18に書込まれた暗号化された情報は、必要に応じて解読するために暗号化装置20に転送される。その後、解読された情報は、プロセッサ16による後続的な使用のために暗号化装置20から読取り／書込みメモリ18に書込まれる。

【００３６】

ハッカーが符号またはセンシチブなデータを彼等自身が目的とするものに修正することを阻止するために、解読された情報が認証されるまで、暗号化装置20によって解読された情報をプロセッサ16が処理することは許されていないことが重要である。したがって、装置10は認証装置22を具備している。解読された情報を認証するために認証装置22が非常に多数の認証アルゴリズムの任意のものを使

用できることは当業者により認識できることであるが、この好ましい実施形態では、認証装置は、解読された全ての情報を認証するために機密キーを使用するＣＢＣ－ＭＡＣ（暗号化ブロックチェーンメッセージ認証符号）アルゴリズムを行う。当業者によって理解されるように、このような認証には、別個に認証されなければならない暗号化された情報の各セクションに対して期待されたＭＡＣ値の情報が必要とされる。以下さらに説明するように、好ましい実施形態において、要求されたＭＡＣ値は、別のロード時間方式が本発明の技術的範囲を逸脱することなく使用されることができるが、スタートアップ時に読取り／書込みメモリ18にインポートされる。認証装置はメモリ18からのＭＡＣ値を使用して、プロセッサ16による使用の前に、解読された全ての情報に関してＣＢＣ－ＭＡＣ認証を行う。

【００３７】

読取り／書込みメモリ18の内容は、バーサクリプト(VersaCrypt)アプレットを実行する過程においてプロセッサ16または別の手段によって更新されていてもよい。解読された情報が再度暗号化され、エクスポートされた場合（以下説明するように）、認証装置22は、現時点で読取り／書込みメモリ18中に現在存在する解読された情報を、その情報ブロックに対する新しいＣＢＣ－ＭＡＣ値を生成することにより再度認証することが重要である。新しいＣＢＣ－ＭＡＣ値は、将来当該情報を解読して再使用することが必要になった場合に、その情報ブロックの認証時に後続的に使用するために読取り／書込みメモリ18に書込まれる。再認証は、少なくともいくつかの例では、プロセッサ16が処理中に解読された情報の内容を変更するために必要である。解読された情報の内容の変更により、その情報ブロックは（高い確率で）異なったＣＢＣ－ＭＡＣ値を有することになるので、ＣＢＣ－ＭＡＣ値が再認証によって更新されなければ、将来更新された情報への呼出しが必要になった場合、認証装置22は当該情報を認証することができない。当業者によって認識されるように、認証されたバージョンは事実上最も新しくエクスポートされたバージョンであることを確認する多数の可能な方法が存在する。このような任意の他の確認方法が本発明の技術的範囲を逸脱することなく使用されることができる。

【００３８】

再認証後、暗号化装置20は、読取り／書込みメモリ18中の解読されて認証された情報を再度暗号化された情報に再度暗号化する。

【００３９】

当業者によって認識されるように、多数の適用において、装置10によって処理されるべき暗号化された情報の量は、装置10の内部メモリ容量を越える。このような環境で装置10が動作できるようにするために、装置10は、暗号化された情報をメモリ24のような外部装置と読取り／書込みメモリ18との間で選択的にインポートおよびエクスポートするためのインポート／エクスポート手段を具備している。しかしながら、当業者は、本発明の技術的範囲を逸脱することなく暗号化された情報がシステム中の内部バスを介してハードドライブあるいは別の記憶媒体または通信デバイスへのランまたはワン・ネットワーク接続によりインポートおよびエクスポートされることが可能なことを理解するであろう。外部メモリ24の記憶容量は、読取り／書込みメモリ18の記憶容量を越えていることが好ましい。インポート／エクスポート手段はプロセッサ16と共同して、情報の暗号化されたブロックを外部メモリ24から必要に応じてインポートする。暗号化された情報は、読取り／書込みメモリ18にインポートされると、上述したように暗号化装置20によって解読され、認証装置22によって認証される。その後、プロセッサ16は解読された情報を処理することができる。プロセッサ16が情報ブロック（少なくとも近い将来の）を終えたとき、解読された情報（実施された任意の処理変更が実施された）は、認証装置22によって再度認証され、暗号化装置20によって再度暗号化され、インポート／エクスポート手段によって外部メモリ24にエクスポートされる。

【００４０】

当業者は、インポート／エクスポート手段が本発明の技術的範囲を逸脱することなく多数の方法で構成可能なことを理解するであろうが、示されている実施形態において、それは１以上の外部接続を有するバスによって構成されている。

【００４１】

当業者によって認識されるように、暗号化された情報が外部メモリ24に記憶

される適用では、予防措置をとらないと、ハッカーが修正されたブロックおよびそのブロックが修正された時機に関する情報を認識することが可能となり、この情報が統計的アタックで使用されることができる。このような情報は、暗号化された情報の著作権を侵害しようとするハッカーを潜在的に助けるものになる。これを回避するために、装置10の暗号化装置20は、ホワイトニングキーに関してキーサイクリングを行うように構成されることが好ましい。

【００４２】

本質的に、ホワイトニングは、数学的動作（排他的オア動作のような）を行ってホワイトニングキーを情報ブロックと組合せ、事実上キー材料をさらに強化する。ホワイトニングプロセスは、暗号化された情報ブロックおよび対応した解読された情報ブロックに関して（すなわち、暗号化が行われる前後の両方で）行われることができる。この技術を示されている装置10において使用する利点は、暗号化された情報ブロックが、解読された情報の内容が変更されたか否かにかかわらず、エクスポートされたときに（前のインポート／エクスポートシーケンスから）常に異なって見えることである。換言すると、示されている装置10において、暗号化装置20は、装置10によって提供された機密の保持された安全な環境において、解読され再度認証された情報がその元の暗号化された形態と異なるようにこれを再度暗号化し、それによって解読された情報の内容が修正されたか否かに関する修正情報をマスクする。したがって、暗号化装置20は、解読された情報に対応した暗号化された情報が外部メモリ24からインポートされた場合に第１の形態を有し、それが外部メモリ24にエクスポートされた場合には、対応した解読された情報が不変のままでも、第１の形態とは異なる第２の形態を有するように情報を暗号化する。この技術のために、暗号文の原文が知られないため、アタッカーは既知の原文アタックの可能性を与えられず、また、アタッカーは暗号文原文の制御を拒否されるので適応選択された暗号文原文アタックの可能性を与えらない。アタッカーは、ホワイトニングキーが各エクスポート動作により変更されたときに、このキーに対して統計的アタックを行うことができず、それゆえキーの寿命は十分に短い。これに関して、当然ながら、たとえばＤＥＳキーのキーサイクリングまたはパッケージ転送を含むその他の方法を使用することができる。

【００４３】

所定の情報ブロックに関して行われる実質的に全ての各インポート／エクスポート動作についてホワイトニング効果が与えられることを確実にするために、暗号化装置20は、ホワイトニングキーに関してキーサイクリングを行うように構成される。とくに、暗号化装置20は、それが暗号化する情報のセクションごとに新しいホワイトニングキーを使用するように構成される。したがって、前にエクスポートされた暗号化された情報のブロックが外部メモリ24からインポートされたとき、前のインポート／エクスポートサイクルにおいて使用されたホワイトニングキーは、解読プロセスで暗号化装置20によって使用される。その後、その同じ情報ブロックがエクスポートされたとき、暗号化装置20は新しいホワイトニングキーを使用して暗号化プロセスのホワイトニング部分を実行する。

【００４４】

当業者によって理解されるように、ホワイトニングキーによってホワイトニングされた情報ブロックを効率的に解読するために、暗号化装置20はホワイトニングキーを有していなければならない。エクスポートされた暗号化された情報のブロックごとに新しいホワイトニングキーが使用されることが好ましいため、ホワイトニングキーを内部に記憶すると、装置10はメモリリソースを急速に奪われる。このような結果になることを避けるために、この好ましい実紙形態では、暗号化されたバージョンのホワイトニングキーは、対応したホワイトニングされた暗号化された情報ブロック中の予め定められた位置に書込まれ、暗号化され、ホワイトニングされた情報ブロックと共にエクスポートされ、外部メモリ24に記憶される。これによって、暗号化された情報ブロックがインポートされたとき、暗号化装置20はブロック中の既知の予め定められた位置からホワイトニングキーを検索し、そのホワイトニングキーを解読プロセスで使用する。暗号化されたホワイトニングキーはブロックの内部に存在しているため、それはそのブロックの残りによる認証によってカバーされることは明らかである。示されている実施形態では、ホワイトニングキーはメモリリソースを保存するために装置10の外部に記憶されるが、当業者は、記憶されたホワイトニングキーをエクスポートされた情報ブロックにマッピングする方式でホワイトニングキーを装置10に内部的に記憶

することにより（上述の認証情報に関して行われたように）、セキュリティレベルを高めることができることを理解するであろう。このようなホワイトニングキーの管理方法は、もちろん本発明の技術的範囲を逸脱することなく使用されることができる。

【００４５】

当業者によって認識されるように、示されている実施形態では、エクスポートされた情報ブロックに対するＣＢＣ－ＭＡＣ値が揮発性の読取り／書込みメモリ18に記憶されるので、電源の故障が生じた場合、あるいは別のあるリセット状態が発生した場合には、メモリ18中のＣＢＣ－ＭＡＣ値は失われる。ＣＢＣ－ＭＡＣ値が失われた場合、認証装置22は、エクスポートされた情報ブロックを再度インポートする時に認証できず、したがって防止措置をとっておかないと、エラー状態が発生する。これらの状況のために、当業者は、故障許容システムのような永久的な記憶装置が修正されたＣＢＣ－ＭＡＣ値のために設けられていない場合、元の暗号化された情報ブロックは保存され、スタートアップ時に元のＣＢＣ－ＭＡＣ値と共に使用されなければならないことを理解するであろう。上述のように、示されている装置10において、元の形態の暗号化された情報ブロックに対するＣＢＣ－ＭＡＣ値は、外部メモリ（たとえば、図３のＲＯＭ142 ）に恒久的に記憶され、メモリ14から読取り／書込みメモリ18にスタートアッププロセスの一部としてロードされる。したがって、装置10がリセットされたときには、常に読取り／書込みメモリ18中のＣＢＣ－ＭＡＣ値もまたそれらの元の値に復元される。その結果、示されている実施形態において、よく知られている信頼できる状態から処理が始まることを確実にするために、処理は常に元の暗号化された情報ブロックから始められる。

【００４６】

当業者によって認識されるように、上記のＣＢＣ－ＭＡＣ値処理方法は、暗号化された情報に対する前の修正が失われることを当然意味している。しかしながら、これは、前の動作の結果が必ず失われることを意味するものではない。その代わりに、不揮発性メモリが記憶している装置10の前の使用時に修正されたデータは装置10から離れた永久的な記憶装置に記憶され、必要に応じてインポート

されることができる。この不揮発性メモリは、情報を用途に応じて暗号化または解読された形態で記憶することができる。暗号化されたフォーマットおよび認証されたフォーマットの少なくとも一方で記憶された場合、このような情報に対する認証情報はある不揮発性メモリにより内部的に記憶されるか、あるいは装置10の外部においてある不揮発性メモリに記憶されて必要に応じてインポートされなければならないが、内部記憶が好ましい。

【００４７】

示されている装置10は、ホワイトニングアルゴリズムと共にトリプルキー、トリプルＤＥＳ－ＣＢＣによって暗号化された情報ブロックの全てを暗号化する。好ましい実施形態において、キーの階層構造が使用される。情報ブロックは、セッションキーを解読キーとしてトリプルＤＥＳによって暗号化される。したがって、セッションキーは、システムによって処理された情報ブロックの任意のものを解読するために必要とされる。セッションキーを得るために、マスターキーにアクセスしなければならない。マスターキーを得るために、デバイスキーにアクセスしなければならない。このようにして、装置10によって生成されたサービス環境をハッカーから保護する際にデバイスキーのセキュリティを維持することが最も重要である。以下詳細に説明するように、デバイス、マスターおよびセッションキーの暗号化されていない形態は、暗号化装置20およびその暗号化装置のキーファシリティにおいてのみ利用可能である。それらは、常にプロセッサ16によってアクセス不可能であることが好ましい。デバイスキーをスクランブルされた形態で記憶し、ここに説明する拡散チェックサムプロセスによってそのキーを保護することが好ましい。

【００４８】

ここで使用されている“ＤＫ”とはデバイスキーを示し、“ＭＫ”はマスターキーを示し、“ＳＫ”はセッションキーを示し、“ＥＭＫ”は暗号化されたマスターキー（すなわち、デバイスキーにより暗号化されたマスターキー）を示し、“ＥＳＫ”は暗号化されたセッションキー（すなわち、マスターキーで暗号化されたセッションキー）を示す。

【００４９】

上述したように、装置10の主なセキュリティ問題は、デバイス10において使用されるキーのセキュリティを保存することである。キーは装置10のどこかのメモリに記憶されなければならない。しかしながら、ハッカーが機密保持された安全な環境を打ち破るためにそのメモリからキー材料を読取ろうとする可能性は高い。したがって、装置10内に記憶されたキー材料のような機密データへのアクセスを制御するための装置を含むことは避けられない。

【００５０】

図３には、装置10のさらに詳細なブロック図が示されている。その図面に示されているように、装置10は、データを記憶するための不揮発性メモリ32と、メモリ34に含まれているデータへのアクセスを制御するための手段とを含むデバイス30を備えている。不揮発性メモリ32は、示されている装置30においてＥＥＰＲＯＭとして構成されている。しかしながら、当業者は、本発明の技術的範囲を逸脱することなくこの目的で他のタイプのメモリデバイスが使用可能なことを容易に理解するであろう。同様に、制御手段は、予め定められた状態が発生した時に予め規定された機能を行うように構成された多数の論理ゲートを含むハードウェア回路のような論理回路34によって構成されることができるが、当業者は、本発明の技術的範囲を逸脱することなく多数の方法で論理回路34を構成できることを容易に理解するであろう。たとえば、好ましい実施形態において、論理回路34はプログラムされたプロセッサ16によって構成される。

【００５１】

論理回路34は、メモリ32にアクセスして、メモリ32に含まれているデータの少なくとも一部分が機密データを含んでいるか否かを決定するように構成されている。論理回路34は、データに固有のプロパティを解析することによってこれを決定する。とくに、示されている装置10において、論理回路34は、予め定められた特性を有するメモリ32中の任意のデータブロックを識別し、カウントする。その後、それはカウントされたデータブロックの数をしきい値と比較する。論理回路34は、この比較の結果を使用して、メモリ32における機密データの存在または不在を示す。

【００５２】

さらに特有の例をあげると、メモリ32に記憶されたデータは、通常そうであるように各ビットが“１”または“０”の論理状態を有している一連のビットによって表される。示されている装置10において、論理回路34は、論理状態“１”を有しているメモリ中のビットの数をカウントするように構成されている。その後、カウントされた数は、予め定められたしきい値数と比較される。この比較によって、論理状態“１”を有するメモリ32中のビットの数がしきい値数を越えることが示された場合、論理回路34は機密データがメモリに記憶されていることを示し、それに対するアクセスを制限する。この比較により、論理状態“１”を有するメモリ32中のビットがしきい値数を下まわることが示された場合、論理回路34は機密データが存在しないことを示し、メモリ32に対するアクセスに課された制限を解除する。予め定められた特性を有するデータブロックを識別してカウントし、カウントされたブロックをしきい値と比較するこのプロセスが、ここにおいて“拡散されたチェックサムプロセス”と呼ばれている。

【００５３】

機密データがメモリ32中に存在するか否かは、メモリ34自身の中のデータの固有のプロパティに基づいて決定されることに注意することが大切である。それとは対照的に、従来技術では、機密データがメモリ中に存在するか否かに関する決定は、メモリに記憶された１以上のフラグビットの状態を読取ることによって行われることが多かった。このような従来技術のデバイスにおいて、フラグビットは、機密データが存在しない場合は第１の状態に設定され、機密データが存在する場合には第２の状態に設定される。これらの従来技術の方法には、メモリに対する完全なロック／ロック解除決定が比較的小さい数のビット（時にはただ１つ）に基づいており、これらのビットは保護されているデータまたはその存在の実表示を構成しないという欠点がある。ハッカーは、たとえばメモリに損傷を与えたり、あるいは偽り読取りを誘導することによりフラグビットの状態を変更することによって、これらの従来技術の方法をしばしば利用しようとする。ハッカーは、フラグビットの状態の変更に成功した場合、機密データが実際にメモリに記憶されているときにこれらの従来技術のデバイスにこのような機密データが存在しないと確信させ、それによって機密データにアクセスすることができる。

【００５４】

示されている装置30では、はっきりと対照的に、ロックとロック解除との決定を制御するフラグビットは存在しない。したがって、メモリ32の小さい部分の内容を損傷し、あるいは変更しても、デバイスのロックを解除するには不十分である。その代わり、適切に低いしきい値が選択された場合には、機密データが存在しないことを論理回路34に確信させるために、メモリ32中のほとんど全てのデータの状態が変更されなければならない。さらに、機密データの存在を識別するために使用されたデータは、機密データ自身であるため、メモリ32のロックを解除するのに十分なこのデータの状態を変更することにより、メモリ32に記憶された実質的に全ての機密データが破壊されることが好ましい。換言すると、メモリ32に記憶されている機密データがないと論理回路34に決定させるのに十分な固有のプロパティの変更は、メモリ32中のデータを破壊する。その結果、適用に対してしきい値が適切に設定されている場合には、アタックを成功させるメモリ中の機密データは不十分でなければならない。換言すると、機密データの決定はある人為的計量ではなく、機密データ自身の存在に関連している。

【００５５】

当業者によって認識されるように、上述した拡散されたチェックサムプロセスは、本発明の技術的範囲を逸脱することなく、メモリ32の全体またはメモリ32の一部分のいずれに関して行われてもよい。さらに、しきい値は、本発明の技術的範囲を逸脱することなく任意の所望の値に設定することができるが、比較的低いレベルに設定されることが好ましいことを当業者は理解するであろう。理想的には、装置のロックが解除される前に全ての機密データが破壊されなければならないように、しきい値は１に設定される。しかし、試験を可能にするために、しきい値を選択する際に、セキュリティと試験可能性との間で妥協がなされなければならない。実際には、示されている装置において、メモリ32の制御された部分は３Ｋビットであり、しきい値は６４ビットに設定される。当業者は、本発明の技術的範囲を逸脱することなく、しきい値を任意の所望のレベルに設定できることを理解するであろう。しきい値は、容認できないほどシステムのセキュリティを妥協しない公開の許容可能なレベルであるものの決定に基づいて選択されるこ

とが好ましい。

【００５６】

さらに、当業者は、示されている装置10において論理回路34によってカウントされたデータブロックが論理状態“１”を有するビットであるが、この論理回路34は本発明の技術的範囲を逸脱することなく、論理状態“０”を有するビットをカウントするように、あるいは２進値の予め定められた範囲内（たとえば、０００００００１０と０００１０００１との間）の２進値のようなあるプロパティを有する複数のビットを含むデータブロックをカウントするように構成されることが可能なことを理解するであろう。

【００５７】

示されている装置10，30に存在する固有の均衡(tension)は、セキュリティに対する必要性と試験可能性および最初のプログラマビリティとの間で行われる。とくに、上述したように、情報ブロックを解読／暗号化するために使用されたキー材料の保存所（すなわち、メモリ32）へのアクセスを制御することが重要であり、また、製品の販売前、ならびに装置10が販売されて現場で使用された後に返品された場合に、そのメモリ32を試験できることが大切である。試験は、しばしばメモリ32の読取りおよび書込みを必要とする。したがって、試験が可能であることは、メモリ32に記憶されたデータの機密性を守るのに不都合である。

【００５８】

示されている装置10において、試験は、上述の拡散されたチェックサム試験により機密データがメモリ32中に存在しないことが示された後でのみ行なわれることができる。

【００５９】

機密データにより既にプログラムされている返品された装置等に関しては、試験は、最初にメモリ32を消去することによってのみ行われることができる。したがって、装置10は、以下説明する制御されたプロセスによりメモリ32の消去をトリガーするための手段を備えている。

【００６０】

消去方法はまた、適用によって所望されるならば、タンパー(tamper)応答と

して使用されることができる。

【００６１】

メモリの部分的な消去をトリガーする（たとえば、消去をトリガーし、その後装置への電源を速やかに落とす）ことによってハッカーがメモリ32内の機密データにアクセスすることを阻止するために、論理回路34は消去トリガーに応答して、メモリ32を最終的な状態に消去する前に１以上の中間値を有する中間データブロックでメモリ32にはじめに記憶されたデータブロックを置換することによってこのメモリ32を消去するように構成される。この中間値は、メモリ32に記憶された固有のプロパティを有するデータブロックの数が、機密データが全て破壊されるまで機密データの存在を論理回路34が示すレベルのままであることを確実にするように選択される。論理回路34は、メモリに記憶された中間データブロックを１以上の最終値を有する最終データブロックにより置換することによって、メモリ32を最終的な状態に消去する。

【００６２】

とくに、示されている装置10，30において、論理回路34はメモリ32を３段階で消去する。第１の段階において、論理回路34は、第１の中間値をメモリ32中の第１の位置グループに書込む。第２の段階で、論理回路34は、第２の中間値をメモリ32中の第２の位置グループに書込む。第３の段階で、論理回路34は、最終的な値をメモリ32中の第１および第２の両位置グループに書込む。第１の中間値は、第１の段階の後、またはそのあいだにメモリ32の消去が終わった場合、メモリ32中に固有のプロパティを有するデータブロックのカウントされた数が機密データの存在を示すように選択されることが好ましい。換言すると、中間値は、固有のプロパティを有する非機密データであるように選択される。機密情報の各半分は、拡散されたチェックサムプロセスの下で機密として情報を分類するのにいずれかの半分が存在すれば十分であることを確実にするために、固有のプロパティを有するように選択される。これが選択されるのは、バルク消去が行われる場合に、機密情報を含まないものとしてデバイスを誤って分類する可能性のある未定義状態にいくつかのメモリがなるためである。各半分の固有のプロパティは、揮発性メモリのある劣化の場合の誤分類を防止するためにしきい値を大幅に越えて

いなければならない。好ましい実施形態において、各半分の中に少なくとも９６のビットが設定されなければならない。ランダムに生成されたキー材料は不偏(unbiased)であり、したがってこの数を容易に満たすので、これは不合理な過度の制限ではない。示されている装置10において、第１および第２の中間値は同じである。それらは、１６進値０ｘ５５に設定される。また、示されている装置10において、第１の段階は、メモリ32中の全ての偶数アドレスに１６進値０ｘ５５を書込むことによって行われ、第２の段階は、メモリ32中の全ての奇数アドレスに１６進値０ｘ５５を書込むことによって行われ、最終段階は、メモリ32中の全てのアドレスに１６進値０ｘ００を書込むことによって行われる。しかしながら、当業者は、本発明の技術的範囲を逸脱することなく、第１の中間値、第２の中間値および最終値の少なくとも１つに対して別の値が選択されることが可能であり、および、または、もっと多くのまたは少ない消去段階が使用可能であることを理解するであろう。ハッカーは時には種々の物理的アタックによってメモリの内容を読取ろうとすることはよく知られている。メモリ32の内容の機密性を維持するために使用されるセキュリティ方法を打破するためにこれらの技術が使用されることを防止するために、種々のセキュリティ方法（たとえば、保護層がメモリ32に物理的に取付けられることができる。）が使用されることができる。

【００６３】

当業者によって理解されるように、上述の拡散されたチェックサム手順は、メモリ32またはメモリを含むシステムのセキュリティ状態を定めるために使用されることができる。拡散されたチェックサムプロセスが機密データの存在を示した場合、メモリ32は、第１のセキュリティ状態であると定められる。機密データが存在しない場合、メモリ32は、第２のセキュリティ状態であると定められる。示されている装置10において、メモリ32の試験は、このメモリ32が第２のセキュリティ状態のときにのみ可能である。

【００６４】

上述のように、示されている装置10は少なくとも２つのセキュリティセル、すなわちカーネルモードセルおよびユーザモードセルを使用する。プロセッサ16は、ユーザモードで非機密ソフトウェアを動作し、カーネルモードで機密ソフト

ウェアを動作することが好ましい。多くの適用に対して、２つのセキュリティセルで十分である。しかしながら、場合によって２つより多くのセキュリティセルを有することが好ましい。たとえば、多数の秘密タスク間における多重タスクが可能であることが望ましく、ソフトウェアを同時に実行する２以上のセル（たとえば、異なったベンダからの異なった条件付きアクセスシステム）間に保護を設けることが望ましく、また、１つのセルを妥協して処理したことによりシステムの全てが犠牲になることを防ぐことが望ましい。

【００６５】

図２に示されているように、示されている装置10は随意に、別個のアドレス空間における多数のセキュリティセルの実施、および機密保持された安全な内部メモリ18と外部メモリＳＤＲＡＭ24との間における要求時ページングを容易にするメモリ管理装置38を備えていてもよい。示されている実施形態において、メモリ管理装置38は、必要に応じて多数のセキュリティセル間においてメモリリソースを割当てる時にプロセッサ16を補助するコプロセッサとして構成される。この適用において、各ページは、別個に独立して暗号化され、認証されたブロックである。さらに、セキュリティセルのいくつかまたは全ては、内部の機密保持された安全な周辺装置への制限されたアクセスを行うようにユーザモードで動作することが可能であるが、依然として保護された機密保持された環境を有していることが理解されるであろう。当業者は、本発明の技術的範囲を逸脱することなく多数のデバイスがメモリ管理の機能を行うために構成可能なことを理解するであろう。とくに、この機能は、標準的なメモリ管理装置によって容易に構成されることができる。

【００６６】

図３に示されているように、プロセッサ16は、東芝製のＲ３９０４チップの中心部を形成するＲ３０００Ａ ＭＩＰＳ ＲＩＳＣ ＣＰＵ（million instructions per second Reduced Instruction Set Computer Central Processing Unit）によって構成される。図３に示されているように、不揮発性メモリ14は、ＲＯＭによって構成されることが好ましく、不揮発性メモリ32は、ＥＥＰＲＯＭによって構成されることが好ましく、読取り／書込みメモリ18は、揮発性データメ

モリ（ＤＭＥＭ）によって構成されることが好ましく、暗号化装置20および認証装置22は、ハードウェア暗号化装置の性能の利点を利用するために、および大部分のブロック暗号化装置が機密ハッシュに適合可能であるという理由から同じ専用ハードウェア回路によって構成されている。しかしながら、本発明の技術的範囲を逸脱することなく暗号化装置20および認証装置22の少なくとも一方をソフトウェアによって構成することができる。デバイスのセキュリティ要求のために暗号化装置のブロック寸法より大きいハッシュが必要とされた場合、暗号化装置20と認証装置22との組合せは許容可能な妥協にならない可能性がある。プロセッサ16は、３２ビットの汎用バス40（ＧＢＵＳ）によってＲＯＭ14、論理回路34およびＤＭＥＭ18と通信し、いくつかの適用では、この汎用バス40は上述したように、暗号化された情報セクションをＤＭＥＭ18とＳＤＲＡＭ24との間でインポートおよびエクスポートするためのインポート／エクスポート手段としても動作する。

【００６７】

ＤＭＥＭ18と暗号化装置20との間における情報ブロックの移動を制御し、図１の適用における衛星転送機能を備えた暗号化装置20を共用するために、装置10は第２のプロセッサ42をさらに具備している。図３に示されているように、第２のプロセッサ42は、暗号化装置20（暗号化モジュール20により、示されている装置10において構成されている）と通信し、また、バス44を介して読取り／書込みメモリ18（示されている実施形態では、ＤＭＥＭ）と通信している。第２のプロセッサ42は、ＤＭＥＭ18に記憶された情報ブロックの解読および再暗号化を開始するように構成されている。示されている実施形態において、第２のプロセッサ42はシーケンサによって構成されている。開示されている実施形態におけるシーケンサ42の存在およびその暗号化装置20への接続は、目的とする用途（図１）によって左右されるものであり、本発明の実施の成功に必要ない。

【００６８】

示されている装置10において、シーケンサ42は、プロセッサ16へのピア(peer)として動作する。プロセッサ16からシーケンサ42への命令の配信を容易にするために、装置10は命令メモリ（ＩＭＥＭ）46を具備している。動作において、プ

ロセッサ16がシーケンサ42にタスクの実行を要求する必要がある場合、それは必要な命令をＩＭＥＭ46に書込み、制御信号をシーケンサ42に送ってＩＭＥＭ46に命令が存在することを示す。その後、シーケンサ42はこの命令をＩＭＥＭ46から読取って実行する。

【００６９】

上述のように、装置10は、プロセッサ16による実行の前に、解読された情報を認証し、暗号化装置20による暗号化の前に情報を再度認証するように機能する認証装置22を具備している。示されている装置10において、認証装置22は、暗号化装置20によって構成されている。

【００７０】

やはり上述されているように、暗号化装置20は、再度暗号化された情報ブロックが常にそれらが解読前にそうであったものと確実に異なるようにするために使用されるホワイトニングキーに関してキーサイクリングを行うように構成されていることが好ましい。キーサイクリング工程に固有の新しいホワイトニングキーを生成するために、装置10は、暗号文に強い疑似ランダム数発生器（ＣＳＰＲＮＧ）に継続的に再度シードする(re-seed) ために使用されるエントロピーソース48を具備している。既存のハードウェア暗号化装置20の性能上の利点を利用するために、暗号化装置20がＣＳＰＲＮＧを構成している。図３に示されているように、エントロピーソース48は、バス44を介してシーケンサ42および暗号化モジュール20と通信している。シーケンサ42は、要求された時に新しいランダム数を発生し、また再暗号化プロセスで使用されるためのホワイトニングキーの生成時にＣＳＰＲＮＧによって使用されるために暗号化モジュール20にランダム数を配信することをエントロピーソース48に要求するように構成されている。

【００７１】

やはり上述されているように、トリプルキー、トリプルＤＥＳアルゴリズムにおいて使用されるキーのいくつかは、メモリ32に記憶される。これらのキーが暗号化装置20およびメモリ32においてのみ利用可能であることを確実にし、またキーがプロセッサ16、シーケンサ42またはそれらが実行するソフトウェア／ファームウェアの任意のものによってアクセス不可能なことを確実にするために、装

置10はキー分離回路50を設けられており、このキー分離回路50が、キー階層構造の基礎的なキーをロードするために論理回路34を暗号化装置20に接続している。とくに、示されている装置10において、キー分離回路50は、必要なキー材料をＥＰＲＯＭ32から暗号化モジュール20に供給するための機構を提供する。キーが別のシステムコンポーネント（ハードウェア、ソフトウェアまたはファームウェア）によってアクセスされることができないことを確実にするために、メモリ32、論理回路34、キー分離回路50および暗号化モジュール20は、閉システムを構成している。

【００７２】

やはり上述したように、外部ピンの状態は、センシチブな情報が機密保持された安全な環境外に露出されることを防止するために、機密保持された内部周辺装置へのアクセス中に強制的に予め定められた状態にされている。このために、装置10は１以上の沈黙モードサイレンシング回路52を備えている。この沈黙モードサイレンシング回路52は論理ゲートを含むハードウェア回路として構成されていることが好ましく、論理ゲートは、バスサイクルが機密データへのアクセスではないと検出した後を除いて、外部ピンを予め定められた状態（３状態のような）にする。この検出は、バス上に現れるアドレスに基づいて行われることができる。このようにして、内部機密データおよびバス非アクティブ状態への両アクセスがマスクされる。その結果、アタッカーは、実行の流れ、命令実行時間、またはデータアクセスの順序のような詳細に基づいた統計的アタックの情報を拒否される。

［バーサクリプトソフトウェアの説明］

セキュリティのために、機密保持されたカーネルは、実時間オペレーティングシステム（ＲＴＯＳ）が装置10により使用されることのできる種々の制限を課す必要がある。以下のリストは、ＲＴＯＳが満たさなければならない要求／制限を含んでいる：

１．文脈切替え--機密保持されたカーネル（ＲＩＳＣ54(16)上で動作する）は、実際の文脈切替え（すなわち、タスク間の切替え）を行うが、そのように動作することを明確に要求された場合のみこれを行う。先取り可能な、および先取

り不能な文脈切替えが共にサポートされる。

２．バーサクリプト文脈切替え補助--ＲＴＯＳは、バーサクリプトアプレットが、別のバーサクリプトアプレットの実行が可能になると考えられるほど十分長く実行した時機を示すようにフラグを設定することを期待されている。最終的な決定は、別のバーサクリプトアプレットが実行可能か否かに基づいて、このような動作がその時点で割込み禁止の状態にある場合に、機密保持されたカーネルによって行われる。

【００７３】

３．システムスタートアップ--機密保持されたカーネルは、システムスタートアップのプロセスと一体的に関連している。ＲＴＯＳが初期状態、そのロード元、あるいはそのロード方法に関して任意の要求を有している場合、それは、機密保持されたカーネルのスタートアップの一部分であるバーサクリプトブートストラップアプレットによって構成されることができる。

【００７４】

４．カーネルモード--機密保持されたカーネルおよびバーサクリプト（すなわち、装置10によって提供された機密保持された環境内で実行されている暗号化されたソフトウェア）は、プロセッサのカーネルモードを単独で使用する。これは次のことを意味する：（ａ）割込み処理--全ての割込みは、機密保持されたカーネルによって処理され、その後ユーザ供給ハンドラのテーブルに送られる；（ｂ）システム呼出し--機密保持されたカーネルへのＡＰＩはSyscall 命令による。ＲＴＯＳは、Syscall （システム呼出し）命令によるシステム呼出しを実行しない可能性がある。（ｃ）エラー処理--バスエラー等の事象はＲＴＯＳに送られない。（ｄ）アドレスマップ--安全でない周辺装置は全てユーザアドレス空間にマッピングされているため、機密保持されたカーネルはそれらへのアクセス時のボトルネックにはならない。

【００７５】

５．低メモリグローバル--ユーザソフトウェアと機密保持されたカーネルとの間で通信するために少量（２５６バイト未満）のグローバル変数が使用されている。ＲＴＯＳが低メモリグローバルを有している場合、それらをこれらと矛

盾しないようにしなければならない。

【００７６】

６．ＲＴＯＳ用のソースコード--ＲＴＯＳは、機密保持されたカーネルに関して実行するように修正されなければならない。

【００７７】

図４は、ＭＩＰＳプロセッサ54(16)で実行しているソフトウェアの種々のクラス間の関係を示す。このモデルともっと伝統的なモデルとの相違は、所定の機能が機密保持されたカーネルを遂行する必要があることである。これらの機能は、（１）セキュリティのために制御されているハードウェアへのアクセス、（２）割込み処理装置のディスパッチ等の、セキュリティのためにとられなければならない全ての機能、および（３）明確で機密保持されたインターフェースを有するためのバーサクリプト環境との通信である。バーサクリプトアプレットは、可変的なアクセスおよびサブルーチン呼出しの両者によって実時間オペレーティングシステムおよびアプリケーションソフトウェアに直接アクセスできるが、機密保持されたカーネルＡＰＩによる通信を行うように制限されている。

【００７８】

大部分のシステム呼出しは、割込み禁止の状態で実行されるが、もっと長い実行時間を有することを期待されているものは、呼出し側（ｃａｌｌｅｒ）のタスクの一部分として割込み可能であるが先取り禁止の状態で実行する。内部メモリ18において利用可能なカーネル文脈の数は限られているため、これはセキュリティ要求である。この先取り禁止状態にする能力は、機密保持されたカーネルによって限られた期間だけ行われる。それはまた、必要ならば、バーサクリプトアプレットによって使用されることができるが、それが実時間性能に及ぼす影響のために使用が避けられる。

【００７９】

また、割込みから復帰したとき、あるいはバーサクリプトエクスポート／インポート動作をサポートする文脈切替えを行ったときに、少量のサイクルがこっそり行われる。このコードは、割込み待ち時間に対する影響を最小にするために割込み可能な状態で実行される（割込みがディスパッチされる前と同じ割込みマ

スク）。所用時間は、カーネルタスクへの文脈切替えを行うオーバーヘッドに比較して十分に短く、したがってシステム性能に対する影響はそれ程大きくないが、しかし、バーサクリプトエクスポート／インポート動作の性能に大きな差が生じる。

【００８０】

カーネルモードソフトウェアは全て、１つの実時間オペレーティングシステムタスクから実行する。それは、機密保持されたカーネル、全てのバーサクリプトアプレット、およびカーネルモードソフトウェアに対して呼出された任意のユーザ機能によって共用されている。それら全てが共通のタスクを共用する理由は、実際にインポートされて実行可能なバーサクリプトアプレット（多くても）が一時に１つしかないためである。それらを多重タクスとしてサポートできるようにするために、実時間オペレーティングシステムは、実行可能としてマークを付けられた多数のバーサクリプトアプレットを必要とするが、エクスポートされたバーサクリプトアプレットへの文脈切替えが行われると直ぐにそれらはブロックし、エクスポート／インポート動作が実行可能となるまで、その状態である。これは、実時間オペレーティングシステムスケジューラが大幅に修正されなければ、バーサクリプトスラッシングを発生させる。このタスクにおいて実行する機密保持されたカーネルの部分は、エクスポート／インポートソフトウェア（その実行は常に、バーサクリプトの実行と互いに排他的である）であるか、あるいは呼出し側タスクの一部分として実行するシステム呼出しに応答する。ユーザ機能は、常にバーサクリプトまたは機密保持されたカーネルによる要求に応じて動作しており、したがってそれは論理的にタスクの実行の一部分である。ユーザ機能は同期呼出しであるため、呼出し側はその終了を待たなければならない。その実行時間が、別のタスクがブロックできるメッセージの送信のようなエクスポート／インポート動作を考慮に入れるのに十分に長いと予測される場合には、別の手段がとられるべきである。機密保持されたカーネルは、カーネルソフトウェアとユーザ機能との間の同期呼出しのサポートを実行する。これの重要な点は、２つのモード間において機密保持された安全な転送が行われ、カーネルの状態が保護されることである。

【００８１】

機密保持されたカーネルは、それが実行不可能な場合、１目盛り（ｔｉｃｋ）のあいだＲＴＯＳルーチンの呼出しを休眠状態にしておく。これには、１つのバーサクリプトアプレットも実行していない時間、およびそれがバーサクリプトエクスポート／インポート動作を行っている時間が含まれる。このために、バーサクリプト要求を実行を開始するまで、あるいは要求されたアプレットをロードするためにバーサクリプトエクスポート／インポート動作がスタートされるまで、１目盛り（ｔｉｃｋ）までの初期遅延が発生することができる。

【００８２】

シーケンサコード（ＩＭＥＭ46から実行された）は、カーネルおよびユーザセグメントに分割される。カーネルセグメントはさらに分割されて恒久的にロードされるセクションにされ、このセクションは、システム機能と、別のカーネルシーケンサアプレットが必要に応じて重ね書きされる第２のセクションとを提供する。

【００８３】

バーサクリプトの使用は、ソフト実時間要求を満足させることを意図したものである。それは、エクスポート／インポート動作の実行に要する長い（何m秒もの）時間のせいでハード実時間要求を満足させることができない。それはこの文脈切替え時間による短い待ち時間を保証することはできないが、開示されている実施形態では、これはエクスポート／インポート動作に対してわずかなパーセンテージのシステムリソースを使用しながら、１秒あたり数十もの要求をサポートすることができる。大部分の要求がバーサクリプトアプレットを１つしか含んでいない場合、エクスポート／インポート動作は回避され、１秒あたり数千（またはそれ以上）の要求が処理されることができる。終了するのに何秒もかかるＲＳＡキー動作等の、これらの要求のいくつかの処理に要する時間をキーの長さに応じて延長できることもまた価値がない。

【００８４】

バーサクリプトへのアプリケーションインターフェースは簡単なＡＰＩによるものであり、このＡＰＩは、各バーサクリプトアプレットが別個の待ち行列に

割当てられる形態で同じまたは多数のバーサクリプトアプレットに対する多数の要求が待ち行列に入れられることを可能にする。これらの要求は、呼出し側に対して非同期的に処理され、結果を処理するために終了した時にユーザ供給コールバック機能が実行され、あるいはこのコールバックは呼出し側のタスクが阻止(block）できる事象を通知することができる。

【００８５】

暗号化装置20が、多数のキーサイズ、すなわち単一のＤＥＳ動作をサポートするならば、トリプルＤＥＳキーへの増加していくアタックから保護するためにインタロックが存在していなければならない。キー階層構造が使用されている場合でも、任意の暗号化されたキーを信用する前にそれらを認証することが重要である。

【００８６】

デバイスがそれ自身のキーを生成するほうが、キーが外部から注入されるより機密保持が安全であることは一般に認められている。デバイスがそれ自身のキー材料を生成する十分な能力を有している場合、そのほうが限られた期間デバイスの外部に知られるよりも安全である。絶対に知られていないものは、漏洩されるはずがない。外に出なかったものは傍受されることはできない。装置10は、外部から観察不可能な方式でソフトウェアを実行することができ、ハードウェアランダム数発生器（ＲＮＧ48）を有している。自己キー発生は、それが行うように設計された動作のクラスの一例である。この能力は、工場の物理的なセキュリティを保つことができない場合に、機密保持されたデバイスをキーによって暗号化する時に非常に重要である。

【００８７】

自己暗号化の１つの可能な方法において、装置10は、それ自身のキー材料を生成するために３つの機密を必要とする。第１の機密は、ＡＳＩＣ工場でプログラムされる出荷キー（ソフトウェアエクスポート／インポートＥＭＫ、トリプルキー、トリプルＤＥＳ）である。第２の機密は、関連したバーサクリプトアプレットを有するＥＳＫ（トリプルキー、トリプルＤＥＳ）であり、それらは全て第２の工場で提供される。第３の機密は、たとえばキーサーバ用のＲＳＡ秘密キー

（大量）である。

【００８８】

キーサーバは、ヴォールト(vault）と呼ばれる第３の物理的に機密保護されたサイトに配置されていることが好ましい。装置10でキーを生成するために、（１）キーサーバ120 および（２）“試験ジグ”122 （図５参照）のようなハードウェアが必要である。キーサーバ120 は、ヴォールト124 内に配置されている。キーサーバ120 は、ネットワーク接続および装置10’実行専用ソフトウェアを有するパーソナルコンピュータ（ＰＣ）として構成されている。衛星Ｉ／Ｆ94は、キー生成中にさらに多くのエントロピーにアクセスするためにハードウェアランダムソース126 に随意に接続される。このアダプタ10’に対するキー材料は、その他任意のアダプタが使用地で危険にさらされた場合、キーサーバ120 のセキュリティを決して危険にさらされないように特有でなければならない。キーサーバ120 は、ファイアウォール132 によってネットワーク128 から隔離されていることが好ましい。

【００８９】

試験ジグ122 は、第２の工場に設けられている。開示されている実施形態において、試験ジグ122 は、それがプログラムされたときに各装置10に接続されるＰＣ（パーソナルコンピュータ）によって構成されている。試験ジグ122 は、あるネットワークインターフェース128 によってキーサーバ120 に接続されている。装置10の衛星Ｉ／Ｆ94はまた、同じ理由からハードウェアランダムソース130に随意に接続される。それはまたファイアウォール132 によってネットワーク128 から随意に隔離されてもよい。

【００９０】

以下、試験ジグ122 中でロードされる装置10のプログラミングを説明する。図６には、このプログラミング工程のステップが示されている。図６において、プログラムされたアダプタ10で発生するアクションは左側に示されており、キーサーバ120 で発生するアクションは右側に示されており、キーサーバ120 と試験ジグ22との間の通信はこのダイヤグラムの中央における矢印で表されている。

【００９１】

装置10は、以下スタートアップ動作で説明するように、外部ＲＯＭから安全にブートする。以下の動作は全て、バーサクリプトアプレットからのものである。全ての通信は、キーサーバ120 におけるバーサクリプトアプレットと、試験ジグ122 においてプログラムされている装置10中のバーサクリプトアプレットとの間のものである。キーサーバ120 のディスクに記憶された全てのデータは暗号化され、キーサーバ120 での危険性／ウィルスから保護されることが好ましい。

【００９２】

第１のアプレットは、実際には公に知られていないが、キーサーバ120 の“公開キー”を含んでいる。ハードウェアランダムソース130 は、ランダムシード材料を更新するために使用される。外部ランダムビットの効果を最大にするために、適用特定回数だけシード材料の更新が行われる。その後、プログラムされている装置10は、トリプルキー、トリプルＤＥＳセッションキーを生成する。このキーは、キーサーバ120 の公開キーにより暗号化され、試験ジグ122 のネットワークインターフェースを使用してキーサーバ120 に送られる。

【００９３】

キーサーバ120 は、ソースＩＰアドレスをチェックすることによってそれが装置10と通信していることを確認する。ソースが公開キーを使用したために、それは装置10と通信していることも知る。キーサーバ120 は、繰り返されるデータアタックまたは汚染され、劣化したランダムソース130 に対して保護するために、このセッションキーを以前（または最後の適用特定回数において）見ていないことを確認する。セッションキーをその秘密キーで解読した後、プログラムされている装置10とキーサーバ120 との間でその後行われる全ての通信はこのセッションキーで暗号化され（Ｏ－ＣＢＣ）、それを確認するためのＳＨＡハッシュを含んでいる。それらはまた、繰り返されるデータアタックから保護するために、この装置10に割当てられた特有の製造番号およびパケットタイプを含んでいる。

【００９４】

その後、キーサーバ122 は、キーサーバのソース126 （それはさらに安全であると考えられる）からのあるランダム数を装置10に送って、装置10におけるシード材料を更新する。それはまた、製造番号のような任意の割当てられた構成、

およびソフトウェアエクスポート／インポートMKを送る。

【００９５】

セッションキーを得るために応答エンティティが秘密キーを知っていなければならないので、装置10はそれがキーサーバ120 と通信していることを知っている。装置10はキーサーバ120 から受取ったランダム数に基づいてそのランダムシード材料を更新し、その新しい５１２バイトのＥＥＰＲＯＭイメージ（以下説明するコンテント）を生成する。装置10はまた、アプリケーションに必要となる可能性のあるその他任意の機密データを生成する。その後、装置はＲＳＡ公開キーをキーサーバ120 に送り、このキーサーバ120 はデータベース134 においてそれらに符号を付け、それらを保存し、符号付きキーを返送する。

【００９６】

その後、装置10は、操作上または法的理由のために共用する必要が生じる可能性のある機密情報をキーサーバ120 に送る。その後、キーサーバ120 は、受信されたエスクロー材料を記録し、装置10にその構成をコミットするように命じる。最後に、装置10は、その内部ＥＥＰＲＯＭ32を再度プログラミングし、それが成功したことを試験ジグ122 に通知することによって応答し、それによって試験ジグ122 は次の装置10の処理に着手することができる。

【００９７】

上記の説明から、当業者は、公開キーにアクセスすることによりキー生成のセキュリティを破壊することが可能であり、チップ工場の者と第２の工場の者とが共謀する必要があることを理解するであろう。これら３つの機密にアクセスされても、システムは依然として外的なアタックを免れる。

【００９８】

ＥＥＰＲＯＭ32は、以下のデータブロックを含んでいることが好ましい。付加的なＥＥＰＲＯＭを必要とするアプリケーションは、機密保持が安全ではない外部ＥＥＰＲＯＭ、デバイス特定キーにより暗号化された（および内部で認証された）外部ＥＥＰＲＯＭ、およびもっと容量の大きい内部ＥＥＰＲＯＭ32の少なくとも１つを随意に使用してもよい。

【００９９】

【数１】

| ビット | 使　用 |
|---|---|
| １０２４ | スクランブルされたデバイスキー。これはキー階層構造の基礎となるキーで、ソフトウェアに直接アクセスすることはできない。 |
| ３２ | スクランブルされたデバイスキーを除く（ソフトウェアはそれを読取ることができないので）、ＥＥＰＲＯＭ32の制限されたブロック上のチェックサムまたはＭＡＣ |
| １９２ | ソフトウェアエクスポート／インポートＥＭＫ（暗号化されたマスターキー、キー階層構造中の第２のキー） |
| １９２ | ＣＳＰＲＮＧランダム数発生器用のキー |
| ３２×２ | ハードウェアランダム数発生器用のシード |
| ［以下のセクションはフィールドプログラム可能なカーネル領域を構成する］ | |
| ６４ | ＣＳＰＲＮＧランダム数発生器用のシード |
| ［ここからユーザスペースが始まる。これは外部ＳＤＲＡＭにコピーされる］ | |
| ３２ | ハードウェア構造 |
| ３２ | この装置の製造番号 |
| ３２ | ソフトウェアエクスポート／インポートＥＭＫインデックス。ソフトウェアをロードした時に正しいＥＳＫが提供できるように、どのＥＭＫが使用されたのかを示すために使用される。 |

【０１００】

［機密保持されたカーネルに関する構成の詳細］

機密保持されたカーネルの主な目的はバーサクリプト環境を提供することであるが、これを行うために以下のような、スタートアップ、割込み処理、文脈切替え、システム呼出し、例外処理、警報状態処理、およびバーサクリプト管理の動作に関与しなければならない。

［スタートアップ］

スタートアップ時、機密保持されたカーネルは、以下の動作のシーケンスを実行する。このシーケンスは、図７においてフローチャートで示されている。

【０１０１】

Ａ．試験装置リセット／ＮＭＩ原因レジスタ

リセット／ＮＭＩ原因レジスタは、警報が原因である可能性のある全てのリセット／ＮＭＩ状態の原因を検出するために使用されるハードウェアである。それが警報状態を含んでいる場合（ブロック144 ）、リセットまたはＮＭＩで、ソフトウェアはある内部周辺装置を使用禁止状態にする。この動作は、付加的な警報が発生したり、あるいはエラー処理を妨害する動作を停止させるためである。デバッグが使用可能にされた場合（ブロック148 ）、実行が内部ＲＯＭ外のルーチンに移行し、原因に関する情報を利用可能にする。しかしながら、システム動作は続行することができない（ブロック150 ）。そうではなく、ＥＥＰＲＯＭ32の位置に示されているように、これが独立型の製品（すなわち、外部プロセッサを有しないセットトップボックス）である場合（ブロック152 ）、装置10は自己リセット動作を行う（ブロック154 ）。これによって、回復可能なエラーの場合、ユーザの介入なしに装置10が動作を続行する。もちろん、回復不可能なエラーの場合は、装置10は無期限に再ブートし続け、したがって原因はなにも容易に認識できない。自己リセットの前に、原因はよく知られている位置に書込まれなければならないので、必要ならば、論理アナライザにより原因が診断されることができる。この装置10が独立型の装置でない（すなわち、第２の外部プロセッサである）場合（ブロック152 ）、全ての動作は停止し、メモリはクリアされず、原因コードが利用可能にされ（ＰＣＩ80、外的に可視なバス動作およびＬＥＤ140 によって）、チップ10は外部リセットを待機する（ブロック156 ）。

【０１０２】

Ｂ．診断ブートおよびハードウェア初期化

重要度または安全性が最小のハードウェアが初期化される。警報状態がない場合（ブロック144 ）、あるハードウェアが初期化され、全てのプロセッサレジスタおよび内部メモリ（ＩＭＥＭ46およびＤＭＥＭ18）ならびにあるグローバル変数がクリアされ（ブロック164 ）、したがって、とくにバルク消去機能が実行された場合には、前のアプリケーションからのデータは公開されない。

【０１０３】

Ｃ．ＥＥＰＲＯＭ動作

バルク消去がトリガーされた場合、上述された３段階バルク消去動作が使用される。

ＥＥＰＲＯＭ32の３Ｋセクションが読取られ、１の密度が計算される。１の密度が６４のしきい値より低い場合（ブロック170 ）、キー材料は存在せず、試験または初期プログラミングを行うことが可能であると想定される。このような状況おいて、あるセキュリティ回路が使用禁止状態にされる（ブロック172 ）。固定パターン（外部ＲＯＭ142 の存在を検出するために使用される）が存在している場合（ブロック174 ）、外部ＲＯＭ142 にジャンプする（ブロック176 ）。外部ＲＯＭ142 が存在しない場合（ブロック174 ）、装置10はロックアップするが、少なくとも外部試験ピンは使用可能である（ブロック178 ）。

【０１０４】

拡散されたチェックサムプロセスによってメモリ32に機密データが存在することが示された場合（ブロック170 ）、ＥＥＰＲＯＭ32の制限されたブロックにおけるチェックサムが計算される（ブロック182 ）。チェックサムが不適切である場合、フェイタル（致命的）エラーが発生する（ブロック184 ）。装置10は、ＥＥＰＲＯＭ22が劣化したため、あるいはこの装置10がタンパーされたために、ロックアップする。チェックサムが適切ならば（ブロック182 ）、ＥＥＰＲＯＭ32から検索された値に基づいて、種々のハードウェア構成が設定される（ブロック186 ）。

【０１０５】

Ｄ．遅延

その後、ある比較的小さい（公称的に１秒の）遅延が発生する（ブロック186 ）。この遅延は、多数の目的のために機能する。最も重要なのは、それによって、アタッカーが長いシステム再ブート中にユーザに気付かれることなく繰り返し（多数のタイプの自動アタックに対する）を行うたびに長い時間を要することである。

【０１０６】

Ｅ．機密保持または重要なハードウェアの初期化

あるグローバル変数が初期化される（ブロック186 ）。バーサクリプトブート

ストラップのロードに備えて、機密保持されたカーネルの恒久的にロードされるシーケンサアプレットおよびそのダミーユーザシーケンサアプレットがＩＭＥＭ46にロードされ、シーケンサ42がスタートされる（ブロック186 ）。また、あるダミーユーザＲＩＳＣコードがロードされる。バーサクリプトブートストラップアプレットのローディングがシステムスタートアップに対してのみ使用される第２のバージョンを維持するのではなく、正常動作の下で使用されるものと同じコードを使用するように、ダミーアプレットおよびＲＩＳＣコードがロードされる。バーサクリプトアプレットをインポートするための正常なカーネル、シーケンサおよびＲＩＳＣコードはユーザコードが存在すると想定し、これと対話する。カーネルシーケンサアプレットはユーザ背景によって呼出されることを期待し、これが従うべき前景ハンドラ（チップの衛星転送機能の一部分）を有していなければならない。カーネルＲＩＳＣコードは、シーケンサ42が終了することを待機しながら、ＲＴＯＳに制御を譲ろうとし続ける。あるユーザナブ（ｎｕｂ）がこれらの機能を処理するために存在していなければならない。

【０１０７】

Ｆ．バーサクリプトブートストラップアプレットのローディング

外部ＲＯＭ142 またはＰＣＩバス78のいずれからバーサクリプトブートストラップアプレットをロードすることが試みられる。全てのバーサクリプトブートストラップアプレットは、３２ビットの外部ＲＯＭ142 からのものでさえ、実行前にＤＭＥＭ18中にコピーされる。外部ＲＯＭ142 は、試験、返品された装置の診断、デバッグ等を行うために、ＰＣＩバス78を使用せずにシステムをブートするために使用されることができる。その存在は、固定オフセットでよく知られているパターンの第１の半分によって検出されることができる（ブロック188 ）。外部ＲＯＭ142 が存在しない場合（ブロック188 ）、装置10はＰＣＩバス78によるブートを試みる（ブロック190 ）。とくに、それははじめに、ＳＣＢがＰＣＩホストから設定される（非０になる）ことを待っている（ブロック190 ）。その後、それはＳＣＢにおいて特定されたブロックをＳＤＲＡＭ中に読取る。パターンの第１の半分が整合しない場合（ブロック192 ）、フェイタルエラーが発生し（ブロック194 ）、制御がブロック146 に戻る。整合が生じた場合（ブロック192

）、ＥＥＰＲＯＭ32からの装置10の製造番号およびソフトウェアエクスポート／インポートＥＭＫインデックスをオフセット８後にＳＣＢ中に再度書込む（ブロック196 ）。パターンの第２の半分が整合しない場合（ブロック198 ）、フェイタルエラーが発生する（ブロック200 ）。

【０１０８】

他のバーサクリプトアプレットとは異なり、ブートストラップアプレットは割込み禁止状態で実行する。これは、それがシステムスタートアップの一部分であり、また、割込み通知を止める前にいくつかの外部デバイスを明示的にリセットすることが必要となる可能性があるためであるが、それは機密保持されたカーネルの技術的範囲を越えている。このバーサクリプトアプレットは、実ブートイメージのブートストラップローディングを処理すると考えられる。これは機密保持されたカーネルを簡単化し、ブートイメージフォーマットが特定のアプリケーションに適合することを可能にし、また、新しい要求が見出された場合には、おそらく変化するものである。この動作の一部分は、バーサクリプトアプレットのような機密保持された機能を扱うメモリ中のある明確に定められた位置を初期化することを含んでいる。

【０１０９】

バーサクリプトブートストラップアプレットの典型的な動作は、（１）バーサクリプト環境を初期化し、バーサクリプトアプレットおよび認証情報をロードすること、（２）ユーザソフトウェアをロードし、これをタンパーチェックすること、（３）ＣＳＰＲＮＧを初期化すること、（４）システム使用のための機密保持されたカーネルの構成を制御するために使用された種々の機密およびユーザ変数を初期化すること、ならびに（５）割込み禁止状態でのユーザモードのコードへの引き渡しを制御することである。全てのレジスタはクリアされる。割込みが禁止状態にされる。これは、割込みがシステムスタートアップの一部分として、割込み通知を止める前にいくつかの外部デバイスを明示的に試験することが必要になる可能性があるためであるが、それは機密保持されたカーネルの技術的範囲外である。レジスタがクリアされ、システムスタートアップ中にそれらの中におそらく残されたセンシチブな材料を保護する。ユーザソフトウェアは、割込み

ハンドラおよびスタックのような機密保護されない機能を扱うメモリ中のある明確に定められた位置を初期化しなければならない。

［割込み処理（および文脈切替え）］

図８には、割込みハンドラをディスパッチし、割込みから戻るプロセスが示されている。

Ａ．割込み処理

全ての割込みハンドラは、ハンドラのテーブルを提供されたユーザによってユーザモードで実行される。割込みからの復帰は、システム呼出しによる。別個の割込みスタックが存在しているが（バーサクリプトに対して要求されるように、また、それ故に、各タスクはネストされた割込みに十分なスタックスペースを割当てる必要がない）、各タスクが規定されるとき、文脈切替えに使用されるスタックスペースの付加的なバイトを割当てている必要がある。

【０１１０】

種々の理由から、文脈はスタックに保存される。それによって先取り可能な文脈切替えは、スタック上に部分的な文脈を既に保存しているはずのタイマー割込みルーチンからトリガーされたときに簡単化される。機密保持されたカーネルは、これが発生すべき論理的な場所であり、それは、ユーザルーチンが機密保持されたカーネルの割込み処理部分によって保存されたレジスタに関する作業をしていなければならないためである。機密保持されたカーネルはまた、この機能をバーサクリプトに関して有していなければならず、実際に高速で実行する。これは、ユーザコードが実行する外部ＳＤＲＡＭ24より内部ＲＯＭ14のほうが高速だからである。文脈をスタック上に配置することは非常に便利である。それは、バーサクリプトのように、全てのタスクがそれら自身のスタックを持たなければならないためである。また、この方式では、機密保持されたカーネルは、基礎をなすＲＴＯＳのタスク制御ブロックまたはその他のデータ構造の情報を全く必要としない。保存されたスタックポインタがタスク制御ブロック中に保存されていることだけが必要である。機密保持されたカーネルに対する文脈の変更は、残っているレジスタ（ユーザコードのために）をスタックに保存し、スタックポインタを切替え、完全な文脈を復元する（バーサクリプトに対して常に行われるように

）だけでよい。

【０１１１】

Ｂ．割込みスタック

システムセキュリティのために、割込み可能状態にされたとき（あるいは、システム呼出しが行われたとき）、ユーザモードコードはユーザスペーススタックを有していなければならず、カーネルモードコードはカーネルスペーススタックを有していなければならない。さらに、カーネルモードコードは割込みハンドラから割込み可能状態で動作されることはできない。これらの要求は、これらの状況下において、現在の文脈がスタック上に保存される必要がある可能性があるために存在する。ユーザがカーネルスタックを有しているならば、このユーザの文脈が保存されるときに、これを使用してカーネルスペースリソースにアクセスすることが可能である。そのカーネルがユーザスタックを有するならば、彼のセキュリティは、彼の保存された文脈を読取って修正することのできる割込ルーチンにより損なわれる可能性が高い。最後に、カーネルモードに対する割込ルーチンからの制限は、ＤＭＥＭ18に同時に記憶されなければならないカーネル文脈の数を制限することである。

【０１１２】

機密保持されたカーネルは、それが維持しなければならない多数の文脈を有している。各バーサクリプトアプレットは、ＤＭＥＭ18（その時点でロードされたバーサクリプトアプレットに対してのみ）または外部ＳＤＲＡＭ24のどちらで暗号化されたかにかかわらず、それ自身のスタック上に１つの文脈を有している。機密保持されたカーネルはまた、エクスポート／インポート動作を行っているあいだに使用される第２の文脈を有していなければならない。それはまた、システム割込み待ち時間を最小にするために、先取り不能であるが、それらが実行に要する時間のために割込み可能状態で実行されるシステム呼出しを処理するための第３の文脈を有している。これらのシステム呼出しは、そうでなければあるシステム呼出しを同時に行っている各タスクに対して文脈が１つづつ要求され、ＤＭＥＭ18中の多数の文脈が要求されるため、先取り不能でなければならない。この第３の文脈はまた、割込みから復帰したとき、または文脈切替えを行ったとき

に、バーサクリプトエクスポート／インポート動作を助けるサイクルをこっそり行う場合に使用される。

【０１１３】

カーネルモード（バーサクリプトアプレットまたは機密保持されたカーネル）コードが動作しているとき、システムは、割込みルーチンに制御を渡す前に、全てのレジスタを保存およびクリアする（これによって、センシチブなデータが保護および隠蔽する）。これによって、４乃至５μ秒の割込み待ち時間（大部分のシステム呼出しまたはＤＭＡによるバス使用のような、割込み禁止状態の期間を含まない）が生じる。実時間ソフトウェアは、この長い割込み待ち時間に耐え、割込みハンドラの書込みを簡単化することが可能でなければならないため、カーネルは、ユーザコードが割込みされたときに、部分的な文脈をスタック上に保存することとなる。これは、カーネルモードより依然として高速であるが、しかし割込み処理にとって十二分なものでなければならない。

【０１１４】

Ｃ．文脈切替え

割込みから復帰したとき、機密保持されたカーネルは、先取り可能な文脈切替えが必要とされていることを示すために使用されたいくつかのグローバル変数をチェックする。これは、スタックポインタが保存されるべき場所のアドレス（おそらく、この時点におけるタスクのタスク制御ブロック中へのオフセット）と、文脈を復元するために新しいスタックポインタをロードすることのできる場所（おそらく、次のタスクのタスク制御ブロック）のアドレスとを含んでいる。この先取りが生じた場合、それは残っている文脈をスタック上に保存し（ユーザタスクのために）、そのスタックから完全な文脈を復元する（それがカーネルに対して常に行うように）。

【０１１５】

Ｄ．バーサクリプトサポート

機密保持されたカーネルは、割込みから復帰する前、文脈切替えを行っているとき、メモリのブロックのコピーおよびカーネルシーケンサアプレットのスケジューリングのようなバーサクリプトエクスポート／インポート動作に関連したあ

る限られた動作（限られた時間を使用する）を行うことができる。これは、先取り可能文脈切替えを少量だけ遅延することができるが、システム性能に大きい影響を与えてはならない。これらの動作は割込み可能状態で実行されるため、それによって割込み待ち時間は生じない。

カーネルに対するユーザルーチンを実行することとなる、あるいはバーサクリプトアプレットと機密保持されたカーネルとの間で共用されることとなる単一のカーネルタスクが存在する。保存されたスタックポインタは偽りの値（全て１）であり、実際の値を公開しているのではなく、またユーザソフトウェアがそれを変更することを可能にするものでもない。実際のスタックポインタは、ＤＭＥＭ18に保存されているか、あるいはエクスポートされるバーサクリプトアプレットのために外部ＳＤＲＡＭ24中で暗号化されている。この単一のタスクは、バーサクリプトアプレットに低い優先度を与えるが、それは、古いアプレットをそのデータと共にエクスポートしたこと、および新しいアプレットをそのデータ共にインポートしたことに関連した、いずれにしても大きい遅延が原因の場合である。全てのカーネルタスクに対するタスクは１つしか存在しない。これは、一時に実行可能なバーサクリプトアプレットが、他のものが外部メモリ24で暗号化されるために１つしか存在しないためであり、また、ある別のタスクの代わりに機密保持されたカーネルが実行すればよいためである。

【０１１６】

実行の速度については、実行するアプレットがこの時点でロードされる場合、それはエクスポートおよび再度インポートされず、このまま実行する。アプレットにより要求されるロードされることとなるデータセグメントが、現時点で実行しているアプレットによってロードされた場合、このデータセグメントはエクスポートおよび再度インポートされ、機密保持されたカーネルを簡単化する。

【０１１７】

先取り可能なバーサクリプトスケジューリングをサポートするために、ＲＴＯＳはバーサクリプトスワップを要求するようにグローバルフラグを設定しなければならない。これは、ＲＴＯＳタイマー割込みルーチンから容易に行われることができる。

【０１１８】

バーサクリプトスケジューリングを行うために使用されるアルゴリズムは、それがカーネルモードでカーネルタスクへの文脈切替えを行うたびにＶＣスワップをチェックする。（１）バーサクリプトスワップが要求された場合、（２）バーサクリプト実行待ち行列で待機している別のバーサクリプトアプレットが存在している場合、（３）バーサクリプトスワッピングがイネーブルされた場合、未決定のバーサクリプトアプレットを実行する代わりに、エクスポート／インポート動作が開始される。エクスポート／インポート動作に含まれる動作のほとんどはカーネルシーケンサアプレットのローディングおよびそれらの実行のスケジューリングを扱う。シーケンサは、実際の暗号化および認証を行うことができる。これらの動作は短時間で終了できるため、割込みから復帰して文脈切替えを行なうときに、これらの動作を行うためのサイクルがこっそり行われる。残りの動作は、終了するのに長時間を要するため、カーネルタスクから実行される。これらの動作は、ＤＭＡＭ18とＳＤＲＡＭ24との間のブロックをコピーし、キャッシュをフラッシュする。この方法のために、バーサクリプトスワップに関連した付加的な３つのラウンドロビンスケジュール遅延が生じている。これら３つのスケジュール遅延は（１）エクスポートを行ってインポートを開始した後にＤＭＥＭ18からＳＤＲＡＭ14にコピーし、（２）アプレットのインポートをチェックし、命令キャッシュをフラッシュし、データセグメントのインポートを開始し、（３）データセグメントのインポートをチェックし、データキャッシュをフラッシュし、アプレット実行を開始するために使用される。

【０１１９】

Ｅ．バーサクリプトエクスポート／インポート

バーサクリプト制御ブロックの目的は、バーサクリプトアプレットおよびデータセグメントを外部メモリに記憶すること、ユーザバーサクリプト呼出しを管理すること、およびバーサクリプト実行待ち行列を維持することである。機密保持されたカーネル中の共通のルーチンの利点を利用可能にするために、アプレットはデータセグメントの特殊な場合として扱われる。

【０１２０】

以下に外部メモリ24中のバーサクリプト制御ブロックのフォーマットを示す

:

【数２】

| ビット | フィールド | 説　明 |
|---|---|---|
| ３２ | リンク | これは、現在実行を待機しているバーサクリプトアプレットの待ち行列にバーサクリプトアプレットを配置するために使用される。 |
| ３２ | 未使用 | ０ |
| ６４ | 待ち行列 | 所定のバーサクリプトアプレットに対する要求の待ち行列の先頭および末尾。 |
| [ここからタンパーチェックが始まる] | | |
| １６ | ＩＤ | 各ブロックに対する特有の非ゼロＩＤ。 |
| １６ | 寸法 | 暗号化されたセクションの寸法（６４ビットＤＥＳブロックでの、非ゼロ）。 |
| １６ | 未使用 | ０ |
| １６ | フラグ | これらフラグはアプレット対サブアプレット対データセグメント、およびアプレットに対する実行状態を区別するためにシステムによって使用される。 |
| [ここから暗号化が始まる。トリプルキー、トリプルＤＥＳ　Ｏ－ＣＢＣ] | | |
| ６４ | プレホワイト | これは、暗号化の前に全ての暗号文の原文との排他的オアされたランダム値である。この値は各エクスポートと共に変化する。 |
| ６４ | ポストホワイト | これは暗号化の後に全ての暗号文と排他的オアされたランダム値でその値は各エクスポートと共に変化する。 |
| ６４ｎ | データ | これはバーサクリプトアプレット（以下説明）またはデータセグメントのいずれかである。 |
| ６４ | チェックサム | これはデータによりタンパーチェックされた領域上のある暗号化されたチェックサムである。<br>[以下説明するように、必ずしもここに記憶されない]<br>装置10は単一のＤＥＳ　ＣＢＣ－ＭＡＣを使用する。キーの選択はセキュリティ問題ではないため、プレホワイトフィールドはこの動作に対するＤＥＳである。<br>ＩＶはそのワードがスワップされた場合にのみプレホワイトフィールドとなる。 |

【０１２１】

装置10は、キー材料を強化するためにホワイトニングを使用する。これは、エクスポートプロセスによって大量の暗号文がアタッカーに与えられるためである

。それはまた、ブロックがエクスポートされるたびに全てのデータが変更され、どのデータが変化しているのか、あるいはどの程度の時間がある動作に要したのかに関する情報をハッカーに与えないことを意味する。全てのバーサクリプトアプレットのはじめの部分はかなり一定であるため、それはまた、既知の暗号文原文をアタックから保護する。最後に、それはまた適応選択された暗号文原文をアタックから保護し、このアタックでは、ハッカーは、彼等が装置10に渡して、アプレットがそのパラメータをロードした直後にエクスポートされるようにする値を選択することができる。

【０１２２】

随意に、バーサクリプトは、セキュリティをさらに強化し、キーの寿命を制限するために各バーサクリプトエクスポートに対するそのキー材料を変更することができる。

【０１２３】

装置10はまた、長期のデータアタック（これは、ネットワーク上で繰返されるデータアタックに類似している）から保護する。このアタックにおいて、各ブロックに対するチェックサムがＤＭＥＭ18において維持され、ロード時に比較されることができるように、バーサクリプトブロックの数を制限することによりバーサクリプトブロックの古い値が後に再び与えられる。バーサクリプトブロック（アプレット＋サブアプレット＋データセグメント）に対する制限は示されている装置10において３２ブロックであり、すなわち２５６バイトである。

【０１２４】

Ｆ．バーサクリプトブロックＩＤ

バーサクリプトブロックＩＤは、０のリザーブされた値以外の任意の１６ビット値であることができる。唯一の制限は、ＩＤの下位の(bōttom)５ビットが所定のシステムに対して特有でなければならないことである。これは、それらがバーサクリプトブロックの種々のテーブルに対するインデックスとして使用されるためである。

【０１２５】

Ｇ．バーサクリプトブロックタイプ

３つの異なるタイプのバーサクリプトブロック、すなわちデータセグメント、バーサクリプトアプレット、およびバーサクリプトサブアプレットが存在している。データセグメントは、バーサクリプトアプレット間で共用されることのできるデータを記憶するために使用される。それらは、バーサクリプトアプレットによってエクスポート／インポートされてもよく、ユーザコードにより使用可能ではない。バーサクリプトアプレットは、ユーザ呼出し可能なバーサクリプト機能である。それらは、呼出し制御ブロックをバーサクリプト制御ブロックの中の待ち行列中に挿入し、バーサクリプト実行待ち行列中にバーサクリプトアプレットを（まだ存在していなければ）挿入するシステム呼出しを介して呼出される。バーサクリプトサブアプレットは、それらが別のバーサクリプトアプレットによってのみ呼出され、ユーザによって直接呼出されることがないことを除いては、バーサクリプトアプレットである。それらは、エクスポート／インポート遅延が大きいが、大きいアプレットを小さいセクションにセグメント化するために使用される。

【０１２６】

多くの例において、バーサクリプトアプレットおよびバーサクリプトサブアプレットの両者をまとめて示すためにバーサクリプトアプレットという用語が使用されている。実際の相違は、以下に説明するように、それらを呼ぶ者の意図に左右される。バーサクリプトアプレットは、正規のＣ呼出し規約を使用するサブルーチンとして呼ばれており、標準的なＣレジスタ使用を観察しなければならない。それらのスタックポインタは、アプレットのブロックの終わりに初期化され、そのパラメータを利用可能な状態で有する。バーサクリプトアプレットは、それらが使用した全ての非一時レジスタのあるものがバーサクリプトリンケージ情報を記憶するために使用されることになるので、その他任意のＣ機能と同様に、それらを保存しなければならない。

【０１２７】

Ｈ．バーサクリプトデータセグメント

データセグメントは、データセグメントをインポートおよびエクスポートし、データセグメントを生成および削除するために４つのシステム呼出しを介してバ

ーサクリプトアプレットにより管理される。バーサクリプトアプレットは、８つのデータセグメントを同時にロードされるようにしてもよく、終了時には、それら（バーサクリプトサブアプレットに対するパラメータを除く）を明示的にアンロードしなければならない。それらがロード（インポート）されたとき、それらのフォーマットは、それらが暗号化されていないことを除いて、外部メモリ（データによってタンパーチェックされた領域）中のものと同じである。

【０１２８】

バーサクリプトデータセグメント中に実行可能な命令を保持することは妥当ではなく、また命令キャッシュは、バーサクリプトデータセグメントがインポートされたときにフラッシュされない。

【０１２９】

データセグメントが、構築時に生成および初期化され、アプレットにおいて初期化コードが必要とされないようにアプレットによりブートイメージ中にロードされるように設定することが可能である。アプレットにそのデータセグメントを自動的にロードさせることも可能であるため、それらは明示的にロードおよびアンロードされる必要はなく、それらはよく知られているアドレスでロードすることが知られている。

【０１３０】

多数のバーサクリプトアプレットが同じデータにアクセスしようとしている場合には、バーサクリプトアプレットはデータセグメント中のデータへの共用アクセス用の任意の信号装置(semaphore) を処理することができる。それらは、使用禁止（ディスエーブル）バーサクリプト先取り可能フラグを、それがバーサクリプトスケジューリングに悪影響を及ぼさない場合に、この機能に対して使用することができる。

【０１３１】

Ｉ．バーサクリプトアプレット

バーサクリプトアプレットは、システム呼出しを介してのみ呼出される。このシステム呼出しは、バーサクリプトアプレットに対して待ち行列中に呼出しＣＢを入れ、これがその第１のエントリならば、そのバーサクリプトアプレットをバ

ーサクリプト実行待ち行列の終わりに追加する。スケジューラは多数のタスク間でＣＰＵ54(16)を共用し、これらタスクの１つが単一カーネルタスクである。次に、カーネルタスクは、そのサイクルをユーザ機能と、機密保持されたカーネルと、実行の準備ができている全てのバーサクリプトアプレットとの間で共用する。バーサクリプトアプレットは先取り可能であるため、長時間にわたって実行する（ＲＳＡのような）単一アプレットは、別のユーザタスクまたはバーサクリプトアプレットの実行が維持されることを阻止する。バーサクリプトアプレットが入力されたとき、それは呼出しＣＢをその唯一のパラメータとして有する。

【０１３２】

バーサクリプトアプレットのような任意の真のタスクは、機密保持されたバーサクリプトアプレットを呼出す安全でないユーザタスクに分割される。たとえば、条件付きアクセスソフトウェアは、スマートカードに対する要求の生成およびスマートカードからの結果の処理を行うバーサクリプト呼出しを行うユーザ部分（スマートカードと通信するための割込みハンドラを含む）を有している可能性がある。ユーザ部分はまた、メッセージ渡し、信号装置および必要ならば周期的な呼出しを処理することが可能である。バーサクリプトは、機密保持されたタスクが関与させられるようにする外部事象を隠すことができないが、代わりに事象の処理を隠蔽しなければならない。

【０１３３】

Ｊ．バーサクリプトサブアプレット

バーサクリプトサブアプレットは、正規アプレットと全く同じであるが、しかしメモリ限界を越えたバーサクリプトアプレットを分解するために使用される。それらは、カーネルのみのシステムの呼出しを介して呼出されることが可能であり、ユーザソフトによって直接呼出されることはできない。それらがバーサクリプトアプレット（またはサブアプレット）によって呼出された場合、呼出し側のブロックおよびサブアプレットは実行を開始する。サブアプレットが呼出されたときにすでに実行している場合、警報がトリガーされる（これは、アプレット間におけるルーチンの共用、およびほとんどの場合あるタイプの再帰を予め除外している）。サブアプレットは、再入不可能である。呼出し側は、ＰａｒｍＩＤ（

データセグメントのＩＤである）を送り、バーサクリプトサブアプレットが入力されたとき、それはこのデータセグメントへのポインタをその唯一のパラメータとして有する。データセグメントは、パラメータを送ると共に結果を戻すために使用される。

【０１３４】

Ｋ．文脈切替えチェック

機密保持されたカーネルは、単一カーネルタスクへの文脈切替えを行った場合には常に次のチェックを行う（図９参照）：

１．バーサクリプト先取り可能要求フラグが設定され、使用禁止バーサクリプト先取り可能フラグがクリアされ、バーサクリプト実行待ち行列が空でない場合、（ａ）使用禁止バーサクリプト先取り可能フラグを設定し、（ｂ）エクスポートするために現在のスタックポインタを保存し、（ｃ）機密保持されたカーネルのエクスポート／インポートスタックポインタをロードし、（ｄ）割込み可能にする（ブロック210 ）。この時点で、機密保持されたカーネルタスクは、エクスポート／インポート動作を行うために実行している。

【０１３５】

アプレットが現在ロードされており（ブロック212 ）、所望のアプレットでない（ブロック214 ）場合、それはエクスポートされる。とくに、アプレットが実行を終了していない（ブロック216 ）場合には、それは実行待ち行列の終わりに追加される（ブロック218 ）。ロードされている各データセグメントに対して、したがってアプレット自身に対して：（ａ）エクスポート用のランダムホワイトニング値が生成され、（ｂ）ＭＡＣが計算されて、ＤＭＥＭ18に保存され、（ｃ）ブロックがホワイトニングによって暗号化され、（ｄ）暗号化され、ホワイトニングされたアプレットがＤＭＥＭ18からＳＤＲＡＭ24にコピーされる（ブロック220 ）。バーサクリプト実行待ち行列の上位から次のアプレットが除去される（ブロック222 ）。

【０１３６】

アプレットがこの時点でロードされていない（ブロック212 ）場合、それはインポートされる（ブロック222 ）。とくに、インポートされたアプレットおよ

びその各データセグメントは、（ａ）ＳＤＲＡＭ24からＤＭＥＭ18にコピーされ、（ｂ）ホワイトニングにより解読され、（ｃ）解読されたブロックに対するＭＡＣが計算されてＤＭＥＭ18中のテーブル中の値と比較され、（ｄ）フラグがチェックされ（すなわち、ブロックが期待タイプのものである等を確認するために）、（ｅ）インポートされたアプレットが現在実行していないサブアプレットである場合は、そのテーブル中の第１のデータセグメントがそのパラメータと置換されて、そのためそれがロードされ、（ｆ）アプレットおよびサブアプレットに対するデータセグメントマップの妥当性がチェックされ、（ｇ）命令およびデータキャッシュがフラッシュされる。

【０１３７】

他方において、アプレットがまさにスタートしている（ブロック214 およびブロック224 ）場合、その文脈が初期化され：（ｉ）その保存されたスタックポインタが設定され；（ii）そのパラメータが待ち行列に入れられた呼出しＣＢ（アプレットに対して）またはデータセグメント（サブアプレットに対して）に設定され、（iii）その復帰レジスタ（＄３１）がアプレット終了を処理するために機密保持されたカーネル中のコードを指すように設定され（これにはまた、呼出しＣＢ（アプレットに対して）または呼出しアプレットＩＤ（サブアプレットに対して）を保存する必要がある）、（iv）そのフラグが更新される（すなわち、それが実行されている）（ブロック226 ）。

【０１３８】

状況が上記の３つのいずれであるか（すなわち、アプレットが現時点でロードされる、アプレットが現時点でロードされていない、あるいはアプレットがロードされて、まさにスタートしている）には関係なく、制御は次に割込み禁止状態にし；保存されたスタックポインタを復元し；使用禁止バーサクリプト先取り可能フラグおよびバーサクリプト先取り可能要求フラグをクリアする（ブロック228 ）。

【０１３９】

その後、制御は、カーネル文脈を復元し、カーネルモードに入る。［実行可能なバーサクリプトアプレッチが１つもない場合には、これは１目盛り(tick)の

あいだＲＴＯＳの呼出しを休眠させておくループになる。]

Ｌ．バーサクリプトアプレットのデータセクションフォーマット

以下にバーサクリプトアプレットのデータセクションのフォーマットを示す：

【数３】

| ビット | フィールド | 説　明 |
|---|---|---|
| ３２ | ＳＰ | 保存されたスタックポインタ…<br>バーサクリプトがエクスポートされたときに使用される。 |
| ８×３２ | Ｄｓｍａｐ | これは現時点でロードされるデータセグメントのマップである。各セグメントの第１の１６ビットはセグメントＩＤである。第２の１６ビットは、それがロードされるオフセットである。セグメントは、任意の未使用の（全て０）エントリが後にある状態でオフセットを減少することによって記憶される。 |
| ３２ｎ | アプレット | これはバーサクリプトアプレット：<br>テキスト、データ、Ｂｓｓおよびスタックである。Ｂｓｓおよびスタックは最初０である。バーサクリプトアプレットへのエントリ点は、このセクションの始めであり、スタックはこのセクションの終りから作業を行う。 |

【０１４０】

Ｍ．バーサクリプトアプレット呼出し制御ブロックフォーマット

バーサクリプトアプレット呼出し制御ブロック（呼出しＣＢ）の目的は、バーサクリプトのユーザ要求を行うための明確に定められたインターフェースを有することである。この呼出しＣＢは、非同期要求を可能にするので、それ故ユーザソフトウェアはバーサクリプトアプレットの比較的遅いスケジューリングを待つ必要がなく、多数の要求を待ち行列に入れることができる。異なったセキュリティレベルで動作している２つのタスク間のインターフェースにおいて多数のセキュリティ問題が発生するため、この簡単化されたインターフェースは、あるタイプのセキュリティ問題が生じる可能性の高い領域を最小化することを助ける。

【０１４１】

以下にユーザバーサクリプトアプレット呼出し制御ブロックのフォーマットを示す：

【数４】

| ビット | フィールド | 説　明 |
|---|---|---|
| ３２ | リンク | このアプレットに対する要求の待ち行列中に呼出しＣＢを追加するため。 |
| ３２ | コールバック | アプレットが終了したときに、呼出すためのユーザルーチン。このコールバックは呼出しＣＢを送る。 |
| ｎ | ａｒｍｓ | これらは、任意の結果を戻すためにアプレットおよびスペースに渡された任意のパラメータである。その寸法は各アプレットに特有であるが、それが制限されることが強く推奨される。セキュリティのために、要求の開始時にパラメータがＤＭＥＭ中にコピーされる必要があり、要求の終了時にその結果が元にコピーされて戻されることが重要である。これは、外部メモリおよびそれに対するアクセスの機密保持されない性質のためである。 |

【０１４２】

［タンパーチェック］

上述した種々のタンパーチェック特徴に加えて、装置10は、集積回路をタンパーチェックする方法をさらに実行する。この方法は、リセット事象の検出時に実行される。このような事象が検出された場合、プロセッサ54(16)は、ＥＥＰＲＯＭ32がアクセスされることができないように、リセット状態に保持される。ＥＥＰＲＯＭ32は、プロセッサ54(16)がリセット状態で保持されているときにはアクセスされることができない。これは、プロセッサが全てのＥＥＰＲＯＭへのアクセスを始めなければならないためである。示されている装置10において、メモリを含む全ての可能な回路は、ＢＩＳＴ（組込み自己試験）によって試験される。プロセッサ54(16)は、これらの試験の実行中リセット状態に保持される。プロセッサ54(16)は、試験される素子がそれぞれＢＩＳＴ試験に合格した場合にのみリセット状態から解放される。試験された素子のいずれかのものがそれらの各試験に不合格となった場合、装置10はタンパーされていると考えられ、それ以上命令が実行されないように、プロセッサ54(16)はリセット状態に保持されるので、ブートアップは発生せず、したがってセンシチブな情報が公開されることはない。

【０１４３】

プロセッサ54(16)はこのプロセス期間中リセット状態に保持されるので、こ

のタンパーチェック方法を実施するための装置をさらに設けなければならない。示されている実施形態において、タンパーチェック方法は、ウォッチドッグ回路88（図３参照）の１つによって行われる。このようにして、タンパーチェック方法は、ハードウェアによって実行され、リセット状態が発生するごとに行われることが好ましい。

【０１４４】

当業者は、ＢＩＳＴ試験トリガーとして使用されるリセットのほかにも、本発明の技術的範囲から逸脱することなく、別の事象（たとえば、周期的に発生する事象）をトリガーとして使用することが可能なことを理解するであろう。周期的な事象がトリガーとして使用される場合、装置は影響を受ける可能性のある素子を隔離して試験することが好ましい。さらに、当業者は、プロセッサをリセット状態に保持することに加えて（あるいは、その代わりに）、本発明の技術的範囲を逸脱することなく、別のタンパー応答特性を使用することができることを容易に理解するであろう。さらに、プロセッサは、本発明の技術的範囲を逸脱することなく試験の開始および実行の少なくとも一方を使用されることができる。

【０１４５】

本発明の好ましい実施形態に関する以下の詳細について注意しなければならない。第１に、好ましい実施形態において、装置10は単一の半導体ダイ中に構成される。

【０１４６】

また、好ましい実施形態において、プロセッサ16は、ユーザソフトウェアがアドレススペースのセクションにアクセスして、特権動作を行うことを禁止するカーネル動作モードを有することとなる。第３に、プロセッサ16を除く全てのバスマスタ、すなわちＤＭＡは、制限された視点（ビュー）を有していなければならない。外部バスマスタは使用できないことが好ましい。

【０１４７】

さらに、アドレスマップは、全ての機密保持された周辺装置がカーネルアドレススペース内に入るように、また、その他全ての周辺装置がユーザアドレススペース内に入るように規定されなければならない。さらに、当業者によって理解

されるように、システムは本発明の技術的範囲から逸脱することなく任意の所望の標準規格または適用特定周辺装置を含むことができる。

【０１４８】

さらに、当業者によって認識されるように、好ましい実施形態にわたって、全ての外部リソースおよびユーザ供給パラメータに関して敵対態勢がとられる。このようなリソースは、アタックの結果として予測できない回数で通知せずに変化すると予測すべきである。正規のアクセスは統計的アタックに情報を提供していると考えるべきである。全てのアドレスは、使用前に有効性をチェックされなければならず、全ての値は、認承および使用の少なくとも一方を行う前に内部メモリにコピーされなければならない。

【０１４９】

本発明の特定の例がここに記載されているが、本発明の技術的範囲はそれに限定されるものではない。逆に、本発明は添付した特許請求の範囲の技術的範囲内に入る全ての構成を事実上あるいは等価な原理の下にカバーする。

【図面の簡単な説明】

【図１】

使用可能な１つの環境において本発明の教示にしたがって構成された装置の概略図。

【図２】

図１の装置の概略図。

【図３】

図１および２の装置のさらに詳細な概略図。

【図４】

装置において使用されるソフトウェアアーキテクチャの概略図。

【図５】

装置をプログラムするための例示的なシステムの概略図。

【図６】

装置のＥＥＰＲＯＭのプログラミングを示すラダーダイヤグラム。

【図７】

装置のスタートアップ動作を示すフローチャート。

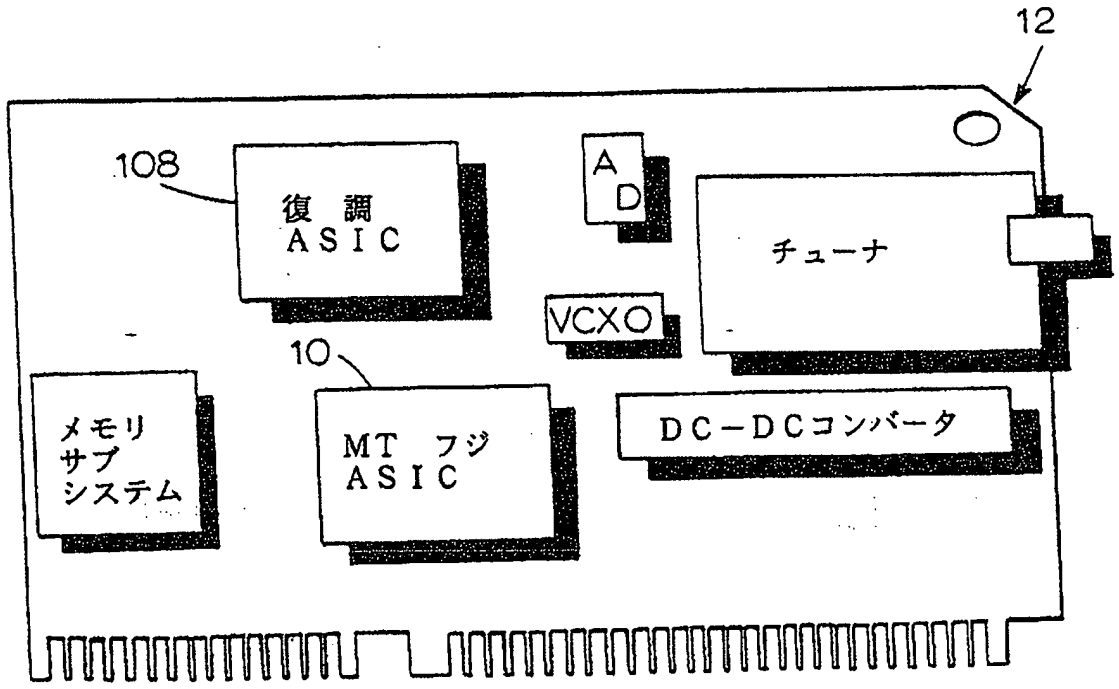
【図８】

装置によって使用される割込み処理プロセスを示すフローチャート。

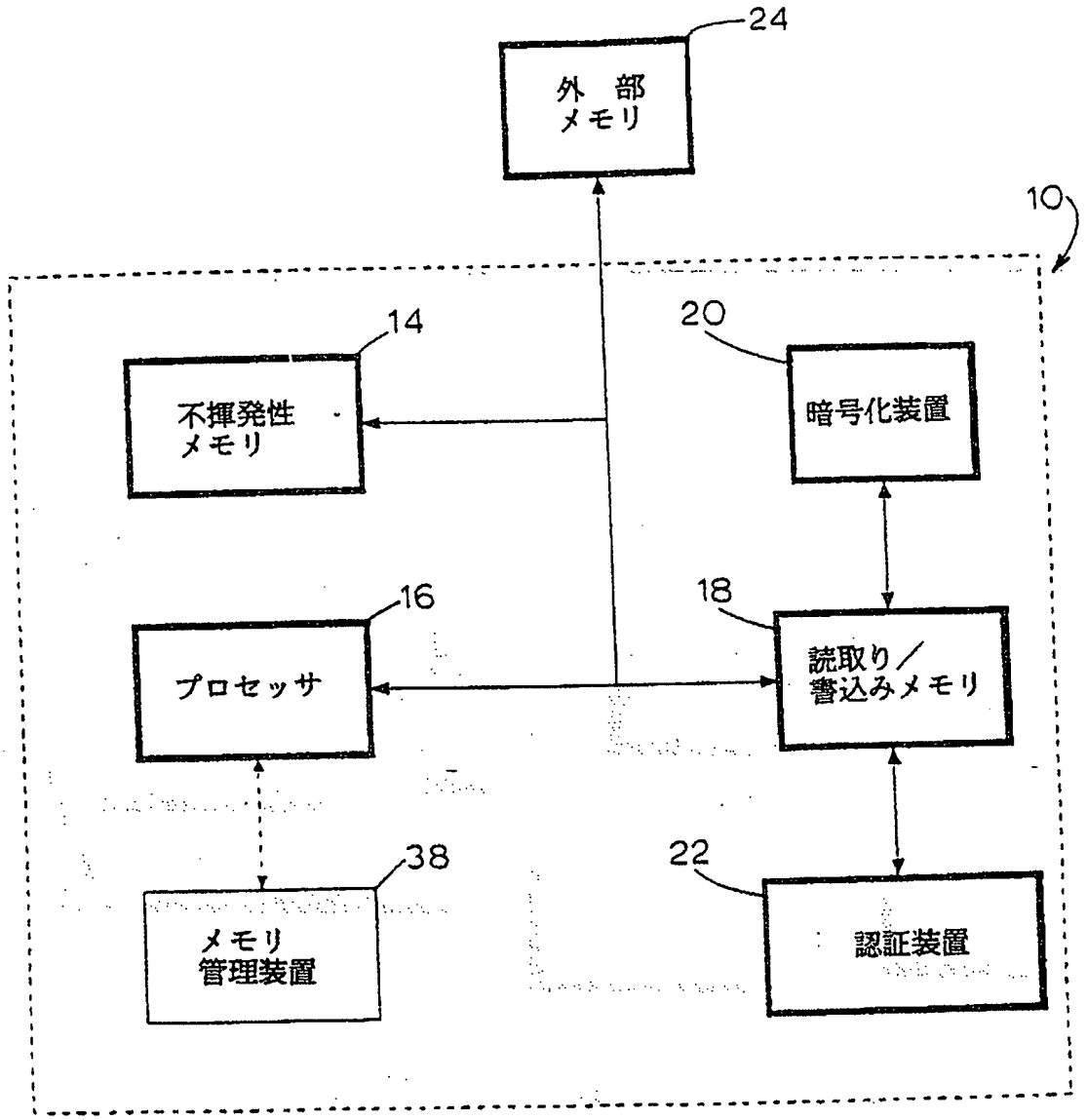
【図９】

外部メモリとＤＭＥＭとの間においてアプレットを交換するために装置によって使用されるプロセスを示すフローチャート。

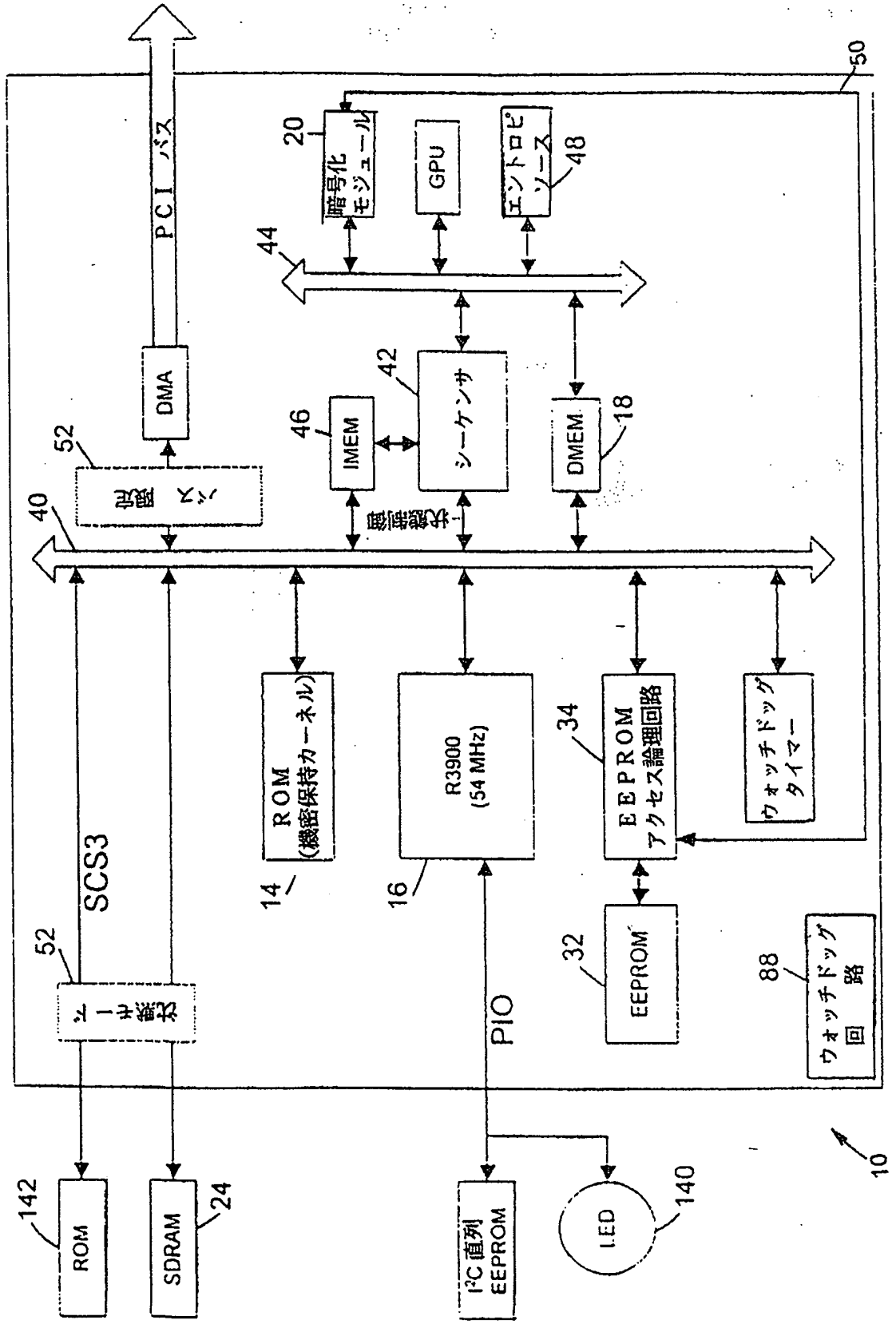
【図１】



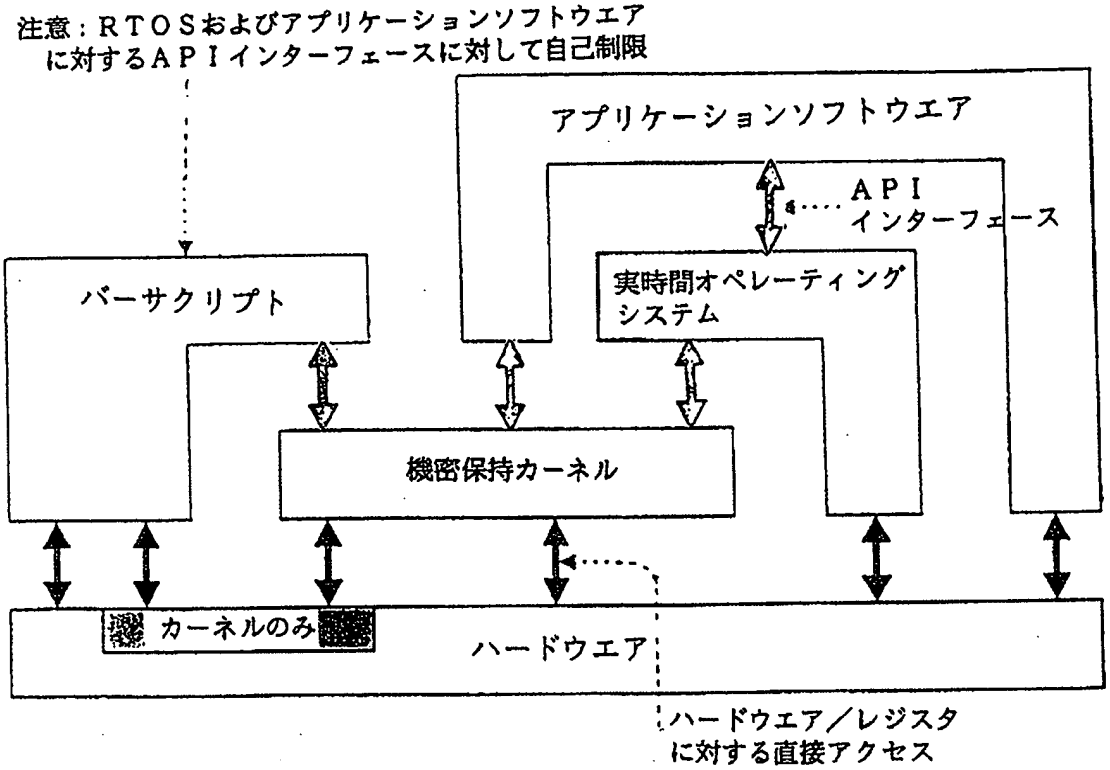
【図２】


24
外 部
メモリ
10
14
不揮発性
メモリ
20
暗号化装置
16
プロセッサ
18
読取り／
書込みメモリ
38
メモリ
管理装置
22
認証装置

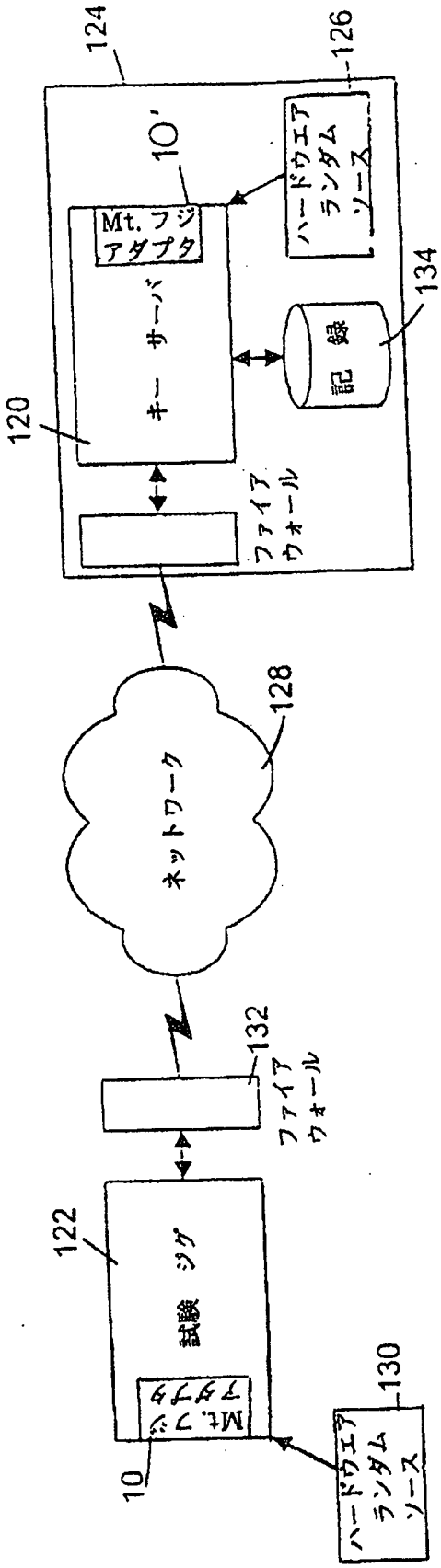
【図３】


PCI バス
50
20
暗号化モジュール
GPU
エントロピソース
48
44
42
シーケンサ
46
IMEM
DMEM
18
DMA
52
バス 調停
40
状態制御
ROM (機密保持カーネル)
14
R3900 (54 MHz)
16
34
EEPROM アクセス論理回路
ウォッチドッグタイマー
SCS3
52
ネットワーク
PIO
32
EEPROM
88
ウォッチドッグ回路
10
142
ROM
SDRAM
24
I²C 直列 EEPROM
LED
140

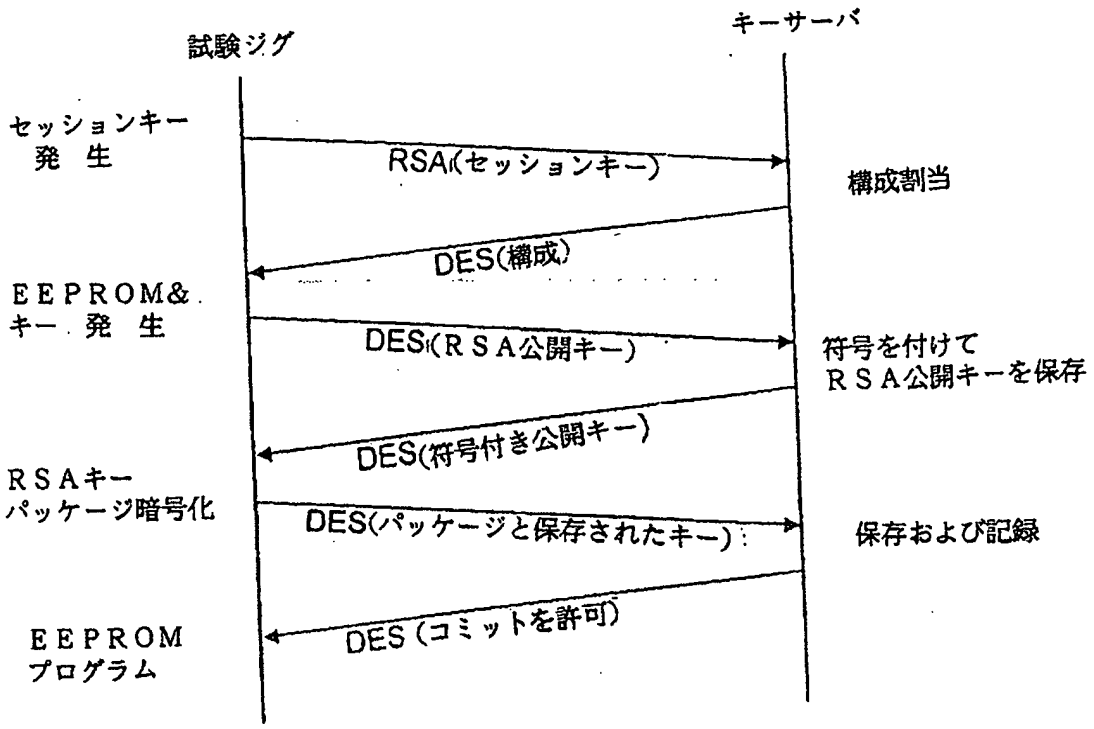
【図４】


注意：ＲＴＯＳおよびアプリケーションソフトウエア
に対するＡＰＩインターフェースに対して自己制限
アプリケーションソフトウエア
ＡＰＩ
インターフェース
バーサクリプト
実時間オペレーティング
システム
機密保持カーネル
カーネルのみ
ハードウエア
ハードウエア／レジスタ
に対する直接アクセス

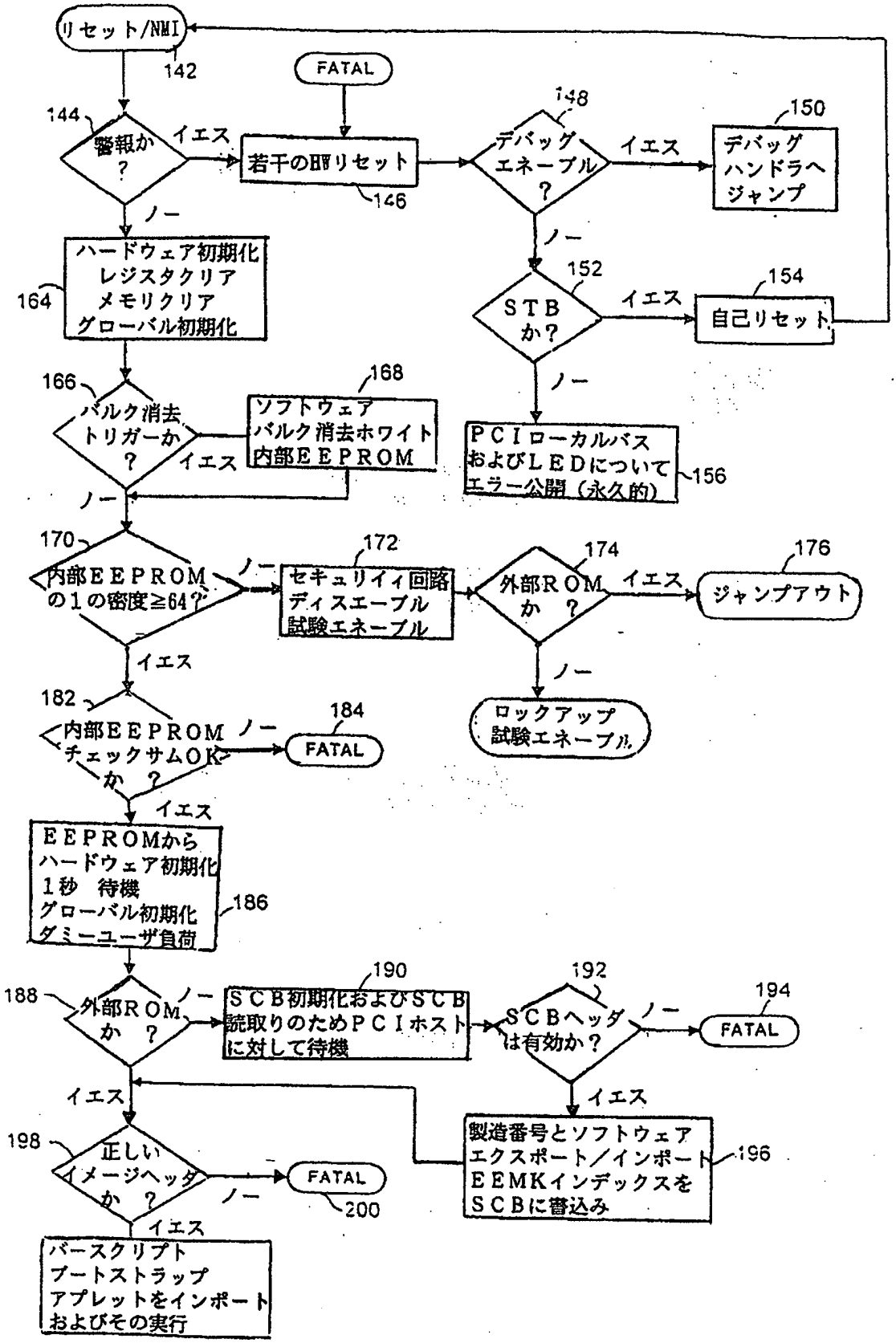
【図５】


124
126
10'
Mt. フジ アダプタ
キー サーバ
ハードウエア ランダム ソース
記録
134
120
ファイア ウォール
128
ネットワーク
132
ファイア ウォール
122
試験 シグ
Mt. フジ アダプタ
10
130
ハードウエア ランダム ソース

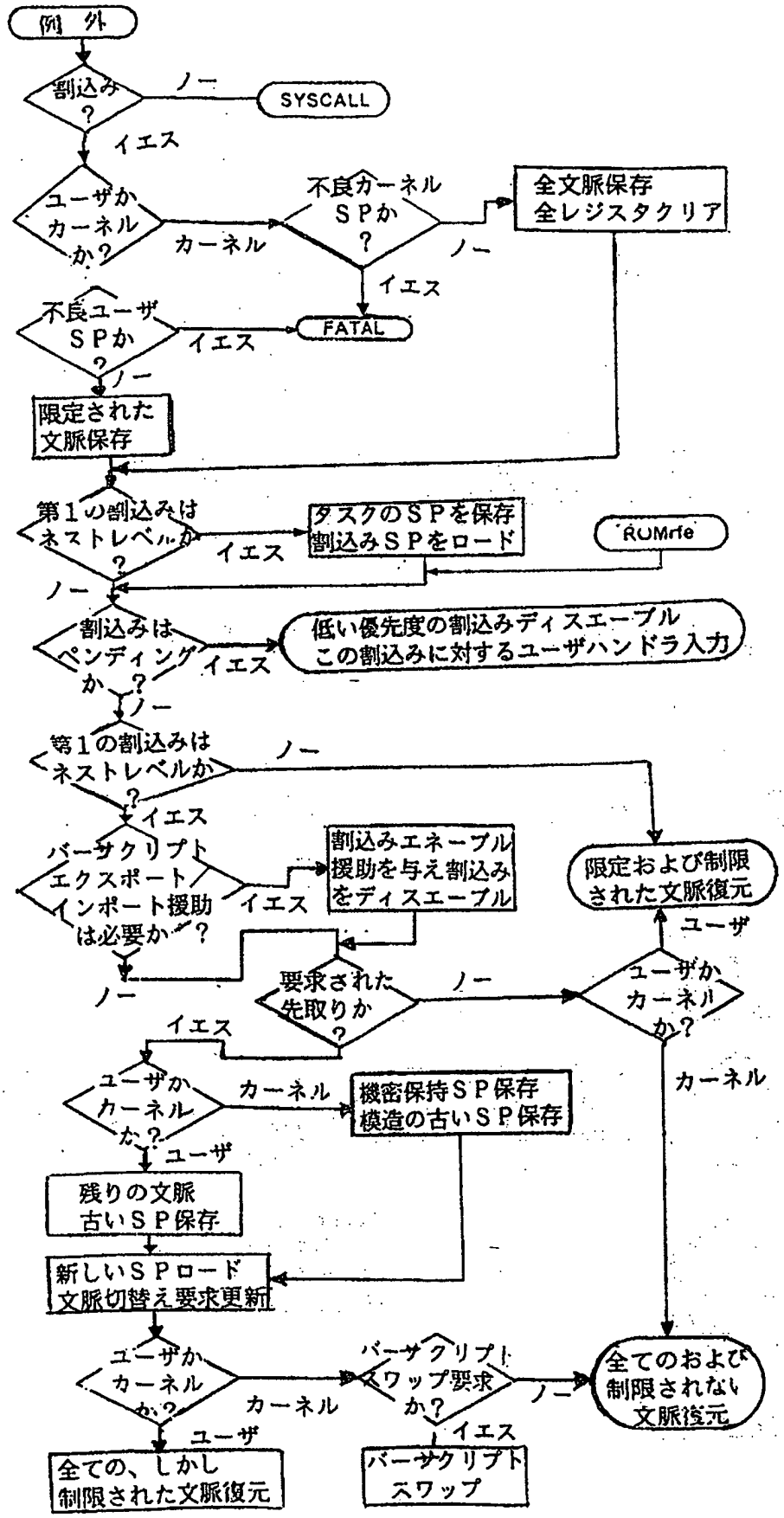
【図６】


試験ジグ
キーサーバ
セッションキー
発　生
RSA(セッションキー)
構成割当
DES(構成)
EEPROM&
キー　発　生
DES(ＲＳＡ公開キー)
符号を付けて
ＲＳＡ公開キーを保存
DES(符号付き公開キー)
RSAキー
パッケージ暗号化
DES(パッケージと保存されたキー)
保存および記録
DES(コミットを許可)
EEPROM
プログラム

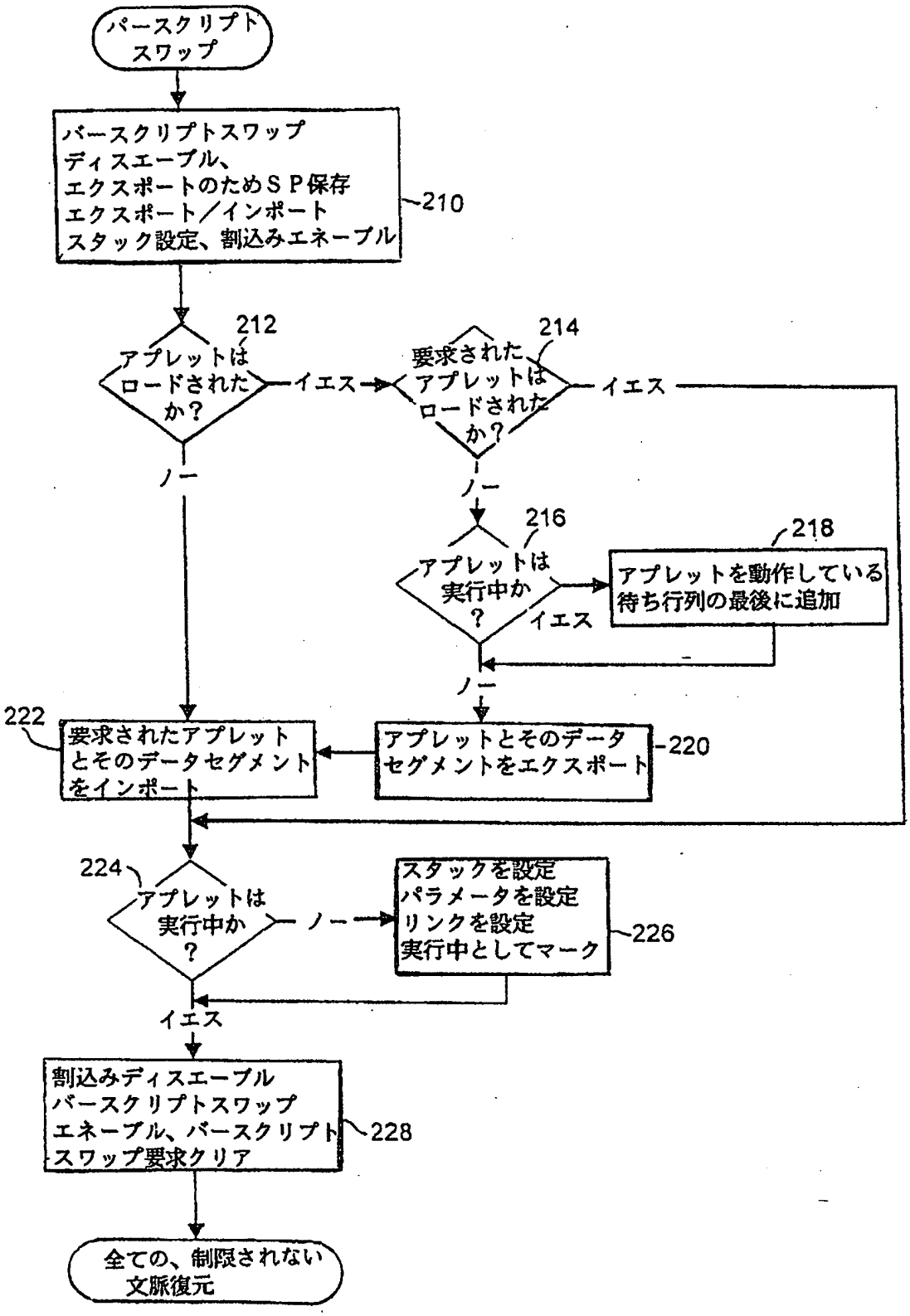
【図７】


リセット/NMI
142
FATAL
144
警報か？
イエス
若干のHWリセット
146
148
デバッグエネーブル？
イエス
150
デバッグハンドラへジャンプ
ノー
ハードウェア初期化
レジスタクリア
メモリクリア
グローバル初期化
164
152
STBか？
イエス
154
自己リセット
ノー
166
バルク消去トリガーか？
イエス
168
ソフトウェアバルク消去ホワイト内部EEPROM
PCIローカルバスおよびLEDについてエラー公開（永久的）
156
ノー
170
内部EEPROMの1の密度≧64？
ノー
172
セキュリィ回路ディスエーブル試験エネーブル
174
外部ROMか？
イエス
176
ジャンプアウト
イエス
ノー
182
内部EEPROMチェックサムOKか？
ノー
184
FATAL
ロックアップ試験エネーブル
イエス
EEPROMからハードウェア初期化
1秒 待機
グローバル初期化
ダミーユーザ負荷
186
188
外部ROMか？
ノー
190
SCB初期化およびSCB読取りのためPCIホストに対して待機
192
SCBヘッダは有効か？
ノー
194
FATAL
イエス
198
正しいイメージヘッダか？
ノー
FATAL
200
イエス
製造番号とソフトウェアエクスポート/インポートEEMKインデックスをSCBに書込み
196
バースクリプトブートストラップアプレットをインポートおよびその実行

【図８】


例外
割込み？
ノー
SYSCALL
イエス
ユーザかカーネルか？
カーネル
不良カーネルSPか？
ノー
全文脈保存
全レジスタクリア
イエス
不良ユーザSPか？
イエス
FATAL
ノー
限定された文脈保存
第１の割込みはネストレベルか？
イエス
タスクのSPを保存
割込みSPをロード
RUMrfe
ノー
割込みはペンディングか？
イエス
低い優先度の割込みディスエーブル
この割込みに対するユーザハンドラ入力
ノー
第１の割込みはネストレベルか？
ノー
イエス
バーサクリプトエクスポートインポート援助は必要か？
イエス
割込みエネーブル援助を与え割込みをディスエーブル
限定および制限された文脈復元
ユーザ
ノー
要求された先取りか？
ノー
ユーザかカーネルか？
イエス
カーネル
ユーザかカーネルか？
カーネル
機密保持SP保存
模造の古いSP保存
ユーザ
残りの文脈古いSP保存
新しいSPロード
文脈切替え要求更新
ユーザかカーネルか？
カーネル
バーサクリプトワップ要求か？
ノー
全ておよび制限されない文脈復元
ユーザ
イエス
全ての、しかし制限された文脈復元
バーサクリプトへワップ

【図９】


バースクリプトスワップ
バースクリプトスワップディスエーブル、エクスポートのためＳＰ保存エクスポート／インポートスタック設定、割込みエネーブル
210
212
アプレットはロードされたか？
イエス
214
要求されたアプレットはロードされたか？
イエス
ノー
ノー
216
アプレットは実行中か？
イエス
218
アプレットを動作している待ち行列の最後に追加
ノー
222
要求されたアプレットとそのデータセグメントをインポート
アプレットとそのデータセグメントをエクスポート
220
224
アプレットは実行中か？
ノー
スタックを設定パラメータを設定リンクを設定実行中としてマーク
226
イエス
割込みディスエーブルバースクリプトスワップエネーブル、バースクリプトスワップ要求クリア
228
全ての、制限されない文脈復元

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

Inter. nal Application No
PCT/US 98/20083

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 262 025 A (FUJITSU LTD) 30 March 1988<br><br>see figures 1,2,4,6<br>see column 2, line 36 - line 56<br>see column 3, line 27 - column 4, line 50 | 1,9-11, 13-17, 21,25, 29,31, 32,36 |
| A | GB 2 205 667 A (NCR CO) 14 December 1988<br><br>see figures 1,3-5,9<br>see page 2, line 4 - page 4, line 6<br>see page 7, line 15 - page 9, line 27<br>see page 11, line 27 - page 13, line 35 | 1,9,10, 13,14,32<br><br>38-42 |

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 23 June 1999 | 30/06/1999 |
| Name and mailing address of the ISA<br>European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Authorized officer<br>Weiss, P |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 98/20083

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ' | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 5 467 396 A (REINER THOMAS C ET AL)<br>14 November 1995<br><br>see figures 1-3<br>see column 5, line 23 - column 6, line 57 | 1,11,12,<br>17-20,<br>29,30,<br>32,38,<br>40,41 |

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/20083

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0262025 A | 30-03-1988 | JP 2086924 C | 02-09-1996 |
| | | JP 8007720 B | 29-01-1996 |
| | | JP 63073348 A | 02-04-1988 |
| | | CA 1298653 A | 07-04-1992 |
| | | DE 3784824 A | 22-04-1993 |
| | | DE 3784824 T | 11-09-1997 |
| | | US 4853522 A | 01-08-1989 |
| GB 2205667 A | 14-12-1988 | CA 1288492 A | 03-09-1991 |
| | | DE 3818960 A | 22-12-1988 |
| | | FR 2616561 A | 16-12-1988 |
| | | JP 63317862 A | 26-12-1988 |
| | | US 4849927 A | 18-07-1989 |
| US 5467396 A | 14-11-1995 | NONE | |

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＵＡ，ＵＧ，ＵＺ，ＶＮ，ＹＵ，ＺＷ

(72)発明者 ディロン、ダグラス・エム
アメリカ合衆国、メリーランド州 20879 ガイザースバーグ、ベル・ブラフ・コート 1

(72)発明者 クロパー、デビッド・エス
アメリカ合衆国、メリーランド州 21771 マウント・エアリー、リーフィー・ハロー・サークル 1012

(72)発明者 ウエーバー、サンドラ・ジェイ
アメリカ合衆国、ペンシルバニア州 15226 ピッツバーグ、ブルックライン・ブールバード 1431

(72)発明者 バウツ、ブランドン・イー
アメリカ合衆国、メリーランド州 20814 ベセスダ、ブリストル・スクエア・レーン 9803

Ｆターム(参考) 5B017 AA07 BA07 CA15
5B076 FC08
5J104 AA08 AA34 NA02 PA14